# Gestão da Segurança de Informação - ISO 27001

Pedro Antunes

December 14, 2021



up201507254
Instructor: Paulo de Carvalho Martins

# Índice

# Resumo

A ISO 27001 é uma norma internacional, que específica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar qualquer sistema de gestão de segurança da informação. Consequentemente, específica os requisitos para os controlos de segurança que devem ser implementados de acordo com as necessidades do sistema e da organização em questão, com o objetivo de mitigarem e gerirem o risco da organização, originando assim um elevado grau de confiança.

A implementação das especificações mencionadas na norma ISO 27001, demonstra que, a organização teve considerações e que tomou medidas para proteger a informação, tentando garantir a confidencialidade, integridade e disponibilidade da informação. Posto isto, a implementação desta norma também permite uma gestão eficaz e uma fácil integração com outros sistemas por seguir uma abordagem à segurança independente de marcas/fabricantes.

Este trabalho foi uma oportunidade para realizar uma auditoria a uma empresa real e tentar perceber as dificuldades e as adversidades envolvidas. Como tal, decidi realizar a auditoria na empresa Pastelaria Prazeres, de forma a entender o nível de segurança da informação presente no contexto da empresa.

Esta pequena empresa possui 3 pastelarias/padarias, uma fábrica para o fabrico de farinhas e pastéis, 4 veículos e escritório com arquivo de documentos. As pastelarias têm sistema de vigilância, rede wifi pública e software de gestão e de faturação certificado.

A informação crítica da empresa são os contratos com os fornecedores de mercadorias e os documentos de faturação ao consumidor final. Muitas vezes, esta informação é transportada em veículos para diferentes locais.

Neste relatório foram avaliados todos os controlos aplicáveis do anexo A para obtenção da certificação ISO27001.

# 1 Avaliação em função da norma ISO 27001

Foi realizada uma avaliação sobre os dez pontos considerados no corpo da norma, sendo os resultados distribuídos por Not Implemented, Partially Implemented and is not documented, Full Implemented and documented e Not Applicable.

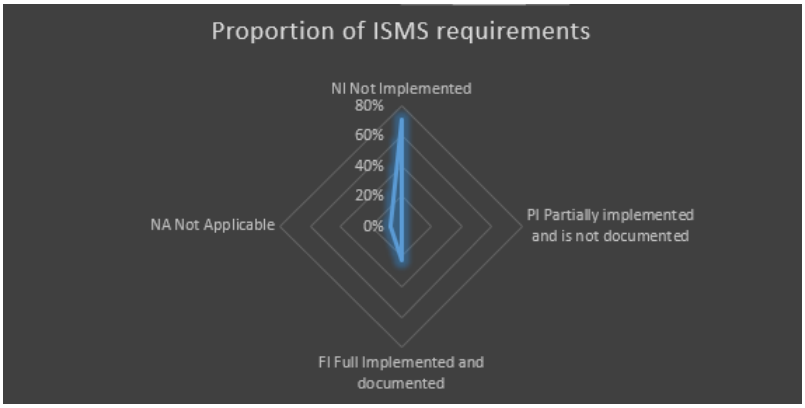


Figure 1: Proporção de requisitos do Sistema de Gestão de Segurança de Informação

O único ponto em conformidade com um Sistema de Gestão de Segurança de Informação sobre o olhar da ISO27001 é o ponto 4 Contexto da organização. o ponto 9 de Avaliação de Desempenho não foi aplicado à empresa. Todos os outros prontos não estão implementados.

## 1.1 Controlos do Anexo A

Em função dos controlos do Anexo A, avaliamos a empresa para perceber quais eram os controlos que estavam implementados, documentados e que se aplicavam à empresa.
O grau de maturidade deve ser visto como um grau de desenvolvimento dos controlos na empresa. Observando a Figure. 2, percebemos que mais de metade dos controlos aplicáveis à empresa não estão desenvolvidos.

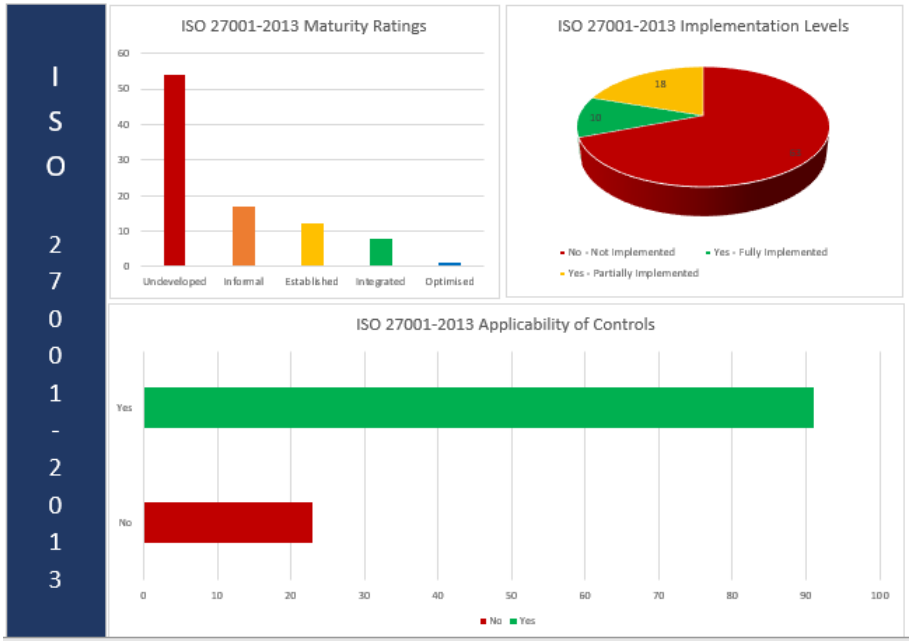


Figure 2: Aplicabilidade, Implementações e grau de Maturidade dos controlos

Os controlos que achei que não se aplicavam à empresa foram:

- A.10 Criptografia;
- A.14 Aquisição, desenvolvimento e manutenção dos sistemas.

Os que controlos que considerei aplicáveis e parcialmente implementados foram:

- A.11 Segurança Física e Ambiental;
- A.8 Gestão de Ativos.

Como opinião pessoal, também achei que a empresa tinha alguns controlos de A.6 Organização da segurança de informação, A.17 Aspetos de Segurança de Informação na gestão da continuidade do negócio e A.18 Conformidade. No entanto, estes controlos precisam de melhorias e documentação para serem considerados implementados.

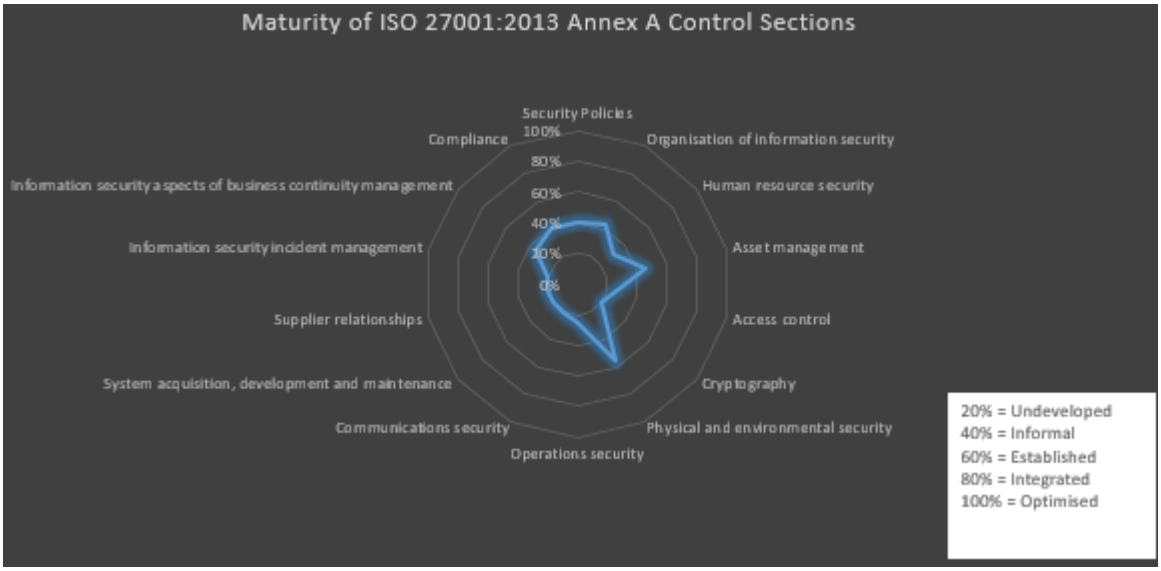


Figure 3: Aplicabilidade, Implementações e grau de Maturidade dos controlos

Os controlos que não estam a ser implementados são todos os restantes:

- A.5 Políticas de segurança de informação;
- A.6 Organização de segurança de informação;
- A.7 Segurança na gestão de recursos humanos;
- A.9 Controlos de acessos;
- A.12 Segurança de Operações;
- A.13 Segurança de comunicações;
- A.15 Relações com os Fornecedores;
- A.16 Gestão de incidentes de segurança de informação;
- A.17 Aspetos de segurança de informação na gestão de continuidade do negócio;
- A.18 Conformidade.

## 1.2 Mitigações de risco

Depois da avaliação feita à empresa de Pastelarias, tentamos elaborar um plano para melhorar a segurança de informação.
Em função do custo de equipamentos e infraestrutura necessária para mitigar certos riscos, foram considerados que alguns controlos do norma não deveriam ser implementados, ficando assim exposto a algum risco.
Seguem-se os controlos que devem ser urgentemente aplicados.

### 1.2.1 A.9 Controlo de Acessos

Devem ser criados controlos de acesso às redes das pastelarias, alterar as credenciais padrão do router e utilizar passwords fortes e complexas.

### 1.2.2 A.13 Segurança nas Comunicações

Devem ser criados controlos de controlo de rede. Com o router corrompido podemos alterar configurações de firewall, port forwarding e redirecionar o tráfego que circula na rede.
Por fim, devem ser criados controlos de segregação de redes. Sem segregação de redes, o computador de faturação fica inserido numa rede pública muito vulnerável.

# 2 Conclusão

Após esta avaliação pormenorizada, podemos concluir que o estado atual da empresa não irá obter certificação ISO27001, pois tem em falha controlos do Anexo A relevantes e fundamentais para assegurar a integridade, confidencialidade e disponibilidade de toda a informação crítica da empresa.