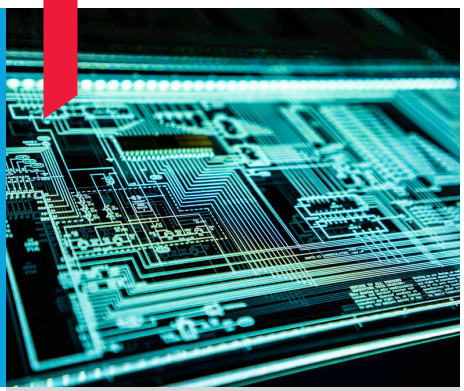
SEGURANÇA DA INFORMAÇÃO

AVALIAÇÃO DA MATURIDADE TECNOLÓGICA COMO PRIMEIRO PASSO PARA A TRANSIÇÃO DIGITAL



Os incidentes cibernéticos são a maior preocupação das empresas em Portugal e no mundo em 2022, de acordo com o Barómetro de Risco Allianz.

Fonte: Allianz Global Corporate & Specialty – Barometer 2022

COMO PODEMOS AJUDAR

A BDO disponibiliza aos seus clientes, sem custos adicionais, uma avaliação da maturidade tecnológica, a alto nível, do sistema de gestão de segurança da informação (SGSI), nomeadamente, através da análise aos processos e documentação que suportam o modelo de governo das tecnologias da informação e a gestão do risco tecnológico da sua organização.

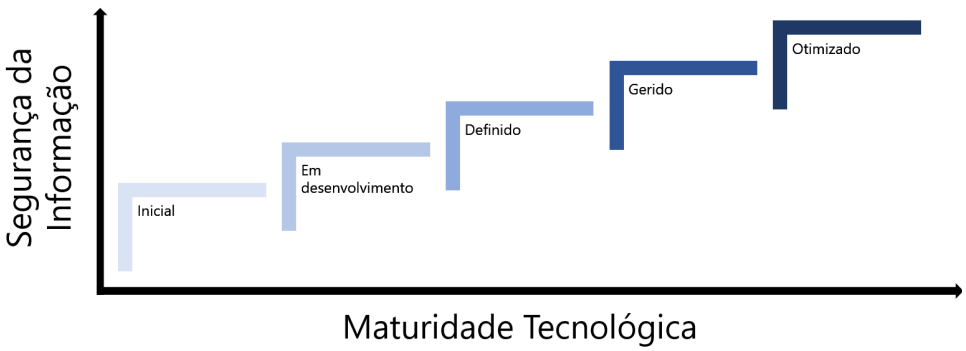
As melhores práticas base para este trabalho são as contidas na norma (ISO/IEC 27001:2013), estruturadas em 14 secções e 114 controlos.

Os níveis da maturidade tecnológica dividem-se em cinco (5) níveis, de Inicial (1) a Otimizado (5) para os três (3) vetores Pessoas/Processos/Tecnologia.

Este trabalho é desenvolvido em duas fases; numa primeira é identificado o nível de maturidade tecnológica alvo, ou seja, o objetivo de posicionamento da organização assim como a sua expetativa temporal.

De seguida, é estabelecido o nível de maturidade tecnológica atual da organização, com recurso à recolha de informação, operacionalizado através de ferramentas colaborativas, numa abordagem de autoavaliação.

Após identificar as duas maturidades tecnológicas, alvo e atual, será elaborado um relatório, composto pelo plano de ações, a alto nível, destinado a sustentar a progressão da maturidade definida.



PARA MAIS INFORMAÇÕES:

ANTÓNIO JORGE PINTO
Manager
Technology Risk and CyberSecurity
+351 937 990 031
antonio.pinto@bdo.pt

MÁRIO SILVESTRE NETO
Partner
IT Services
+351 937 997 003
silvestre.neto@bdo.pt

www.bdo.pt

Este trabalho será efetuado por especialistas em Risco tecnológico da BDO, em sede de reunião remota ou presencial com os responsáveis pelas Tecnologias da Informação da organização.

Apresentamos de seguida um exemplo do relatório de Avaliação da Maturidade Tecnológica a emitir no âmbito deste serviço:

MODELO DE RELATÓRIO DE AVALIAÇÃO DA MATURIDADE TECNOLÓGICA

O relatório de avaliação da maturidade tecnológica da **[Organização]** é suportado pelas melhores praticas contidas na norma ISO/IEC 27001:2013, sendo caraterizada por uma análise, a alto nível, do SGSI (sistema de gestão de segurança da informação), nomeadamente, pela avaliação da existência, atualidade e melhoria dos processos e documentação de suporte. O modelo de avaliação está estruturado em cinco(5) níveis, de Inicial (1) a Otimizado (5).

Preliminarmente, foi definido o nível de **maturidade tecnológica alvo**, o objetivo para a evolução da maturidade tecnológica, que se situa em **Otimizado (5) + Certificação ISO/IEC 27001:2013 no espaço de um (1) ano**.

Esta avaliação da maturidade tecnológica foi operacionalizada em tecnologia Microsoft 365, no modo de auto-avaliação.

Como resultado da avaliação, o nível de **maturidade tecnológica atual** situa-se em um **(1) "Inicial"** caracterizado por uma ausência de processos definidos e as políticas e procedimentos não se encontram documentados nem existem evidências da execução dos processos nem da melhoria contínua, adicionalmente, não existe gestão do risco tecnológico e o conhecimento existente nas equipas é empírico.

Resumo dos níveis da maturidade tecnológica atual:

- Secções relacionadas com a organização: (A.5, A.6., A.8, A.15) - **(1) "Inicial"**
- Secção relacionada com os recursos humanos: (A.7) - **(1) "Inicial"**
- Secções relacionadas com as TIs: (A.9, A.10, A.12, A.13. A.14, A.16, A.17) - **(1) "Inicial"**
- Secção relacionada com a segurança física: (A.11) - **(1) "Inicial"**
- Secção relacionada com a conformidade: (A.18) - **(1) "Inicial"**

De forma a atingir o objetivo da organização, nível **Otimizado(5) + Certificação ISO/IEC 27001:2013**, no espaço de um (1) ano, sugere-se a adoção da seguinte estratégia:

1. Desenvolver um modelo de governo das tecnologias da informação baseado em ISO/IEC 27001:2013;
2. Desenvolver um processo de gestão do risco tecnológico;
3. Dotar as Tecnologias da Informação da capacidade necessária ao atingir dos objetivos;
4. Identificar e disponibilizar o investimento necessário ao atingir dos objetivos.