DEPARTAMENTO DE ENGENHARIA MECÂNICA E INDUSTRIAL

ANA SOFIA MARQUES LOPES DE MATOS
Mestrado Integrado em Engenharia e Gestão Industrial

GESTÃO DO RISCO E CONFORMIDADE EM TECNOLOGIAS DA INFORMAÇÃO SEGUNDO A ABORDAGEM GRC

MESTRADO EM ENGENHARIA E GESTÃO INDUSTRIAL

Universidade NOVA de Lisboa
Setembro, 2021

DEPARTAMENTO DE ENGENHARIA MECÂNICA E INDUSTRIAL

GESTÃO DO RISCO E CONFORMIDADE EM TECNOLOGIAS DA INFORMAÇÃO SEGUNDO A ABORDAGEM GRC

ANA SOFIA MARQUES LOPES DE MATOS
Mestrado Integrado em Engenharia e Gestão Industrial

Orientador: Doutor Izunildo Fernandes Cabral, Professor Auxiliar Convidado da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Júri:

Presidente: Doutora Ana Paula Ferreira Barroso, Professora Auxiliar da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Vogais: Doutora Maria Celeste Rodrigues Jacinto, Professora Associada da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa
Doutor Izunildo Fernandes Cabral, Professor Auxiliar Convidado da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

MESTRADO EM ENGENHARIA E GESTÃO INDUSTRIAL

Universidade NOVA de Lisboa
setembro, 2021

Gestão do Risco e Conformidade em Tecnologias da Informação
Segundo a Abordagem GRC

AGRADECIMENTOS

Um agradecimento formal ao Grupo EDP - Energias de Portugal pela partilha do seu conhecimento e filosofia que permitiu a realização da presente dissertação.

Agradeço ainda ao orientador da presente dissertação pela disponibilidade que demonstrou e por toda a ajuda que ofereceu, esta foi imensamente apreciada.

“Eu sou mais eu"
(Maria José Lopes)

RESUMO

Num ambiente em mudança, o sucesso de uma organização tornou-se intimamente relacionado não só com a sua capacidade de proteger informação valorizada e sensível como com a sua capacidade de gestão do risco. Deste modo, o Grupo EDP - Energias de Portugal, como empresa que enfrenta estes desafios tecnológicos, pretende implementar uma abordagem consolidada nos processos de *Governance, Risk and Compliance* (abordagem GRC) atuando, assim, na unidade de gestão do risco da empresa. Assim, a presente dissertação tem como objetivo desenvolver uma metodologia para suportar a implementação da abordagem GRC segundo o caso de estudo ocorrente no Grupo EDP. De forma a atingir este objetivo recorreu-se à metodologia de *Failure Mode and Effects Analysis* (FMEA) para efeitos de estruturação inicial e desenvolvimento lógico das relações entre os potenciais modos de falha existentes, primeiramente na Digital Global Unit do Grupo EDP, devido ao incumprimento regulamentar, a eficiência dos controlos relacionados e para efeitos de demonstração e comparação de resultados. No âmbito deste estudo foi ainda desenvolvido um plano com base no ciclo *Plan-Do-Check-Act*. Este foi ainda relacionado com a metodologia FMEA. Por último, configurou-se o *software* ServiceNow como forma de automatização da metodologia desenvolvida. Este *software* possibilita o acompanhamento contínuo, através de índices de desempenho dos controlos, dos recursos tecnológicos da organização e garante a sintonia entre a legislação regulamentar interna, as estratégias do negócio e os riscos enfrentados pelo Grupo EDP.

A agregação de todos os benefícios gerados pela abordagem implementada leva a que a área de segurança de TI aplique ferramentas estratégicas adequadas ao alcance dos objetivos delineadas para o sucesso do Grupo EDP anteriormente em falta. Ferramentas estas que permitem a centralização dos dados, a responsabilidade pelos riscos assim como a percepção financeira, probabilística e consequencial dos mesmos, a noção do nível de conformidade legal e do estado atual da organização para diversas frentes incluindo todas as geografias.

No decorrer da implementação da metodologia desenvolvida encontraram-se pequenas limitações referentes à capacidade do *software* ServiceNow. No entanto, uma limitação é destacada, sendo esta, a inaptidão de avaliação, por parte do *software*, do parâmetro de deteção dos controlos. Sugere-se, portanto, a reconfiguração do módulo de risco do ServiceNow de forma a ter em conta todos os âmbitos de avaliação defendidos pela metodologia FMEA.

Palavras-chave: Gestão do risco em TI, Cibersegurança, Abordagem GRC, FMEA, PDCA

ABSTRACT

In a changing environment, an organization's success has become closely dependent not only to its ability to protect valuable and sensitive information but also to its ability to manage risk. Along these lines, the EDP Group - Energias de Portugal, as a company facing these technological challenges, intends to implement a consolidated approach in the processes of Governance, Risk Management and Compliance, the GRC approach, thus acting in the management unit of the company's risk. Hence, this dissertation aims to develop a methodology that aspire to implement the GRC approach according to the case study occurring at the EDP Group. In order to achieve this goal, the Failure Mode and Effects Analysis methodology was used for the purposes of initial structuring and logical development of the relationships between the potential existing failure modes, starting with the Digital Global Unit of EDP, due to regulatory non-compliance, the efficiency of related controls and for purposes demonstration and comparison of results.

Within the scope of this study, a plan was also developed based on the Plan-Do-Check-Act cycle, which was also related to the FMEA methodology. Finally, the ServiceNow software configuration was used as a way of automating the developed methodology. This software enables continuous monitoring, through indices of control performance, of the organization's technological resources and ensures the harmony between internal regulatory legislation, business strategies and the risks faced by the EDP Group.

The aggregation of all the benefits generated by the implemented approach leads the IT security area to apply appropriate strategic tools to achieve the objectives outlined for the success of the EDP Group, which were previously missing. These tools allow the centralization of data, responsibility for risks as well as their financial perception, probabilistic and consequential consciousness of them, the notion of the level of legal compliance and the current realistic state of the organization for several fronts including all geographies.

During the implementation of the developed methodology, irrelevant limitations were found regarding the capacity of the ServiceNow software. However, one limitation was highlighted, this being the inability of the software to evaluate the control detection parameter. Therefore, it is suggested that the ServiceNow risk module be reconfigured in order to take into account all the assessment scopes defended by the FMEA methodology.

Keywords: IT Risk Management, Cybersecurity, GRC Approach, FMEA, PDCA

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

CAE - Conselho de Administração Executivo
COBIT - Objetivos de Controlo das Tecnologias da Informação
D - Deteção
DFMEA - FMEAs de Design
DGR - Direção de Gestão do Risco
DGU - *Digital Global Unit*
EBITDA - *Earnings before Interest, Taxes, Depreciation and Amortization*
FCF - *Free Cash Flow*
FMEA - *Failure Mode and Effects Analysis*
G - Gravidade
GRC - Governação, Risco e Conformidade
IEC - *International Electrotechnical Comnion*
ISMS - *Information Security Management System*
ISO - *International Standard Organization*
ISR - Risco de Segurança da Informação
KPI - *Key Performance Indicators*
MQ - *Magic Quadrant*
NIST - Instituto Nacional de Normalização e Tecnologia
O - Ocorrência
PDCA - *Plan-Do-Check-Act*
PFMEA - FMEAs de Processo
RA - *Risk Assessment*
RBDM - *Risk-Based Decision-Making*
RIDM - *Risk-Informed Decision-Making*
RPN - Número de Prioridade de Risco
SIEM - *Security Information and Event Management*
TI - Tecnologias da Informação
TIC - Tecnologias de Informação e Comunicação

1. INTRODUÇÃO

1.1. Contextualização

Num ambiente em mudança, o sucesso de uma organização tornou-se intimamente relacionado com a sua capacidade de gerir riscos. À medida que as empresas se tornam cada vez mais dependentes da informação para vantagem competitiva própria e a informação ganha ainda mais proporção no valor acrescentado incorporado nos produtos e serviços das empresas, a capacidade de proteger informação valorizada e sensível tornou-se uma capacidade estratégica para garantir a sustentabilidade, a rentabilidade e o valor global de uma empresa (Hohan, 2015). A crescente variedade de ameaças e ataques de cibersegurança fazem da proteção dos ativos da informação um desafio complexo. Garantir a segurança da informação torna-se uma condição necessária para o progresso sustentável da organização devido a razões como a manutenção da vantagem competitiva, a proteção da reputação da empresa e o cumprimento das leis e regulamentos aplicáveis (Kaufmann, 2017).

Atualmente a segurança na área das Tecnologias da Informação (TI) é um assunto fulcral. Tendo em conta que a digitalização inicia o seu caminho para o novo normal e que o funcionamento base da maioria das empresas e organizações está assente em sistemas informáticos indispensáveis para o funcionamento fluído das mesmas, podem, por isso, ocorrer novas formas de comprometimento que interferem com a rotina de produção das empresas (Torabi et al., 2016). Estas podem ocorrer através da exploração *online* de dados privados, perdas de acesso, roubo de informação, indisponibilidade de serviços, ameaças contra a confiabilidade de infraestruturas críticas como redes elétricas, entre muitas outras. O caso do ataque ao Grupo EDP, que teve lugar no dia 13 de abril de 2020, foi um caso de roubo de informação (Prado, 2020). A empresa foi, portanto, alvo de um ataque informático à sua rede corporativa. Este evento condicionou o normal funcionamento de uma parte dos serviços e operações da organização visto que o ataque atingiu o sistema global do Grupo EDP e não uma unidade de negócio em particular (Vinha, 2020). Para conter os efeitos do ataque, onde vários computadores foram infetados com *malware*, aplicaram-se prontamente medidas de prevenção e proteção dos sistemas de suporte de operações como desligar acessos VPN, estes permitem o acesso à rede da empresa por via remota, como sucede com o teletrabalho (Prado, 2020). Devido a estas e muitas outras situações que ocorrem numa base regular e sem fronteiras, todo o desempenho, trabalho e reputação de uma organização podem ser afetados. Podem ainda

existir consequências fatais que prejudiquem a continuação da normal atividade tanto das organizações como da sociedade no geral (Sahebjamnia et al., 2018).

A gestão do risco em TI, a cada dia, constitui parte significativa dos investimentos das empresas que aplicam tecnologia da informação nos processos de tomada de decisão e na implementação dos processos de negócio (Marston et al., 2011). Simultaneamente, também na literatura, esta temática tem merecido a atenção de diversos invertigadores cujos trabalhos assentam no desenvolvimento de modelos ou abordagens cujo objetivo final é lidar com os inúmeros riscos e ataques à segurança digital. Estas abordagens baseiam-se principalmente na estratégia Risk-Based Decision Making (RBDM), embora a estratégia Risk-Informed Decision-Making (RIDM) represente o atual estado da arte (Laine et al., 2021). As diferentes interpretações de uma correta gestão do risco em TI tem sido centradas na quantificação tradicional dos riscos e nos princípios de decisão custo-benefício (Vidmar e Perkovič, 2018; D. Zhang et al., 2013). Uma correta abordagem e aplicação da gestão do risco em TI permite proteger os diversos ativos da empresa, controlar atividades, tarefas e processos, monitorizar controlos e verificar a *compliance* com a legislação de modo a que a exposição aos riscos identificados seja reduzida ou até mesmo eliminada (Grey, 1995).

De forma a obter certificação da conformidade atual, em termos de gestão do risco, é necessário dar resposta às exigências da norma ISO 9001, mais precisamente ao mencionado no ponto "6.1 - Ações para abordar riscos e oportunidades" do documento. Este defende que as empresas devem determinar os respectivos riscos gerais e oportunidades de acordo com o contexto das atividades da organização. Devem ainda identificar, implementar e acompanhar as ações necessárias de abordagem aos mesmos. No caso concreto da temática da presente dissertação, a ISO/IEC 27001:2013 é uma norma para sistemas de gestão da segurança da informação publicada em outubro de 2005, com foco na gestão do risco em TI. A norma tem como princípio geral a adoção, pela organização, de um conjunto de requisitos, processos e controlos com o objetivo de mitigar e gerir adequadamente a segurança da informação da organização (ISO 27001, 2013).

A gestão dos riscos em TI inclui, assim, um conjunto de metodologias que permitem atingir um equilíbrio entre a priorização dos riscos e o custo-benefício dos mesmos. Os riscos em TI são, portanto, apreciados como riscos operacionais, relacionados com a *performance* de qualquer sistema ou serviço de TI dentro de uma empresa (Bristow et al., 2013). O objetivo da gestão dos riscos concentra-se na eliminação, mitigação, transferência ou aceitação dos riscos, tendo em conta os níveis de impacto e probabilidade de ocorrência dos mesmos. As empresas, no geral, pretendem, então, assegurar o conhecimento, em tempo real, das ameaças, vulnerabilidades e consequências que enfrentam, possibilitando, assim, um processo de tomada de decisão informado e ajustado às suas necessidades (Sahebjamnia et al., 2015).

1.2. Descrição do Problema

A gestão do risco em TI na empresa EDP – Energias de Portugal tem como objetivo minimizar o eventual impacto negativo resultante da materialização dos riscos, ao nível da

empresa e dos seus *stakeholders*. Tal atividade engloba um conjunto de práticas de identificação, análise, avaliação, tratamento e reporte dos principais riscos, em linha com as boas práticas internacionais de *governance* do risco, em conformidade com os requisitos legais e regulatórios e correspondendo às expectativas e exigências dos *stakeholders* internos e externos do Grupo.

A avaliação integrada do nível de risco do Grupo EDP é feita por meio do modelo de análise *bottom up*. Este é complementado pela utilização de um modelo *top down*. A organização faz ainda uso de uma solução usual de monitorização de eventos associados aos riscos em TI. *Security Information and Event Management* (SIEM) é, assim, o sistema de gestão e correlação de eventos utilizado. Com a implementação desta solução é possível executar a correlação de diversos dados provenientes de inúmeras fontes dentro de uma grande empresa subdividida em áreas de negócio e unidades de trabalho, como o caso do Grupo EDP. Ao permitir uma centralização e normalização da informação recolhida, é possível detetar anomalias nos sistemas da organização através de regras e filtros e emitir alertas para as mesmas. Cabe à equipa responsável pela gestão dos incidentes de cibersegurança analisar e reagir a estes alertas gerados pelo SIEM.

Existem, no entanto, limitações no sistema de gestão do risco em TI em utilização no Grupo EDP, nomeadamente a impossibilidade da comunicação efetiva e direta do risco para os gestores da organização e a recolha constante de nova informação gerada pelos vários pontos separados da empresa, o que pode conduzir a uma desatualização quase imediata da biblioteca de dados, retirando, assim, o propósito da tecnologia SIEM. Acrescenta-se ainda, como limitação, a falta de coneção entre a regulamentação interna, como as políticas e normas do Grupo, não só com os riscos associados ao não cumprimento das mesmas, mas também em relação aos ativos afetados e aos controlos existentes, assim como a efetividade, responsabilidade e implementação dos mesmos.

Assim, é necessário implementar uma nova abordagem que permita a harmonização, comunicação, atualização, conformidade, centralização e melhoria contínua entre os vários setores das empresas, com o objetivo de melhorar a produtividade das equipas de segurança e a sua resposta aos novos desafios constantes que, na área de segurança de TI de uma empresa, ocorrem a um ritmo praticamente diário (Hunt, 2014).

Existem vários modelos com o objetivo de alcancar uma gestão do risco apropriada. A norma de referência para a segurança da informação ISO/IEC 27001:2013 sugere a utilização de auditorias como ferramenta de melhoria contínua de um sistema de gestão de risco em TI. No entanto, não só é baseada num processo especificado ao cumprimento legislativo, ou seja, verificação da conformidade, como também depende diretamente das características individuais do auditor, da qualidade do procedimento e do regime temporal em que este é efetuado. A prática da aplicação de modelos de avaliação de maturidade, uma abordagem igualmente usada para propósitos de gestão do risco, têm também as suas limitações. Existem quatro modelos de avaliação de maturidade que, no geral, pretendem fazer uma descrição capacitativa referente a comportamentos e processos organizacionais. O objetivo destes é obter resultados fiáveis sobre o alcance do cumprimento de requisitos previamente definidos. Contudo, a procura de melhoria contínua e resposta a novos desafios é inexistente a partir do momento em

que os requisitos definidos são cumpridos. Existe, ainda, depedência das ações ou atividades de trabalho em linha direta com os compromissos selecionados pelo que os resultados podem ser enviesados perante o contexo da situação empresarial.

Face aos desafios que o Grupo EDP enfrenta hoje em dia e tendo em conta as fraquezas inerentes às condutas praticadas de gestão do risco em TI, pretende-se, implementar uma abordagem nova aos modelos utilizados. A presente dissertação propõe e explora uma metodologia de implementação da abordagem *Governance, Risk and Compliance* (GRC) acompanhada pela metodologia de Análise de Modo e Efeito de Falha (FMEA). A esta acrescenta-se, ainda, a configuração do *software* ServiceNow como forma de automatização e atualização instantânea da informação da abordagem selecionada.

1.3. Objetivo

Para dar resposta às limitações atuais da gestão do risco em TI identificadas no Grupo EDP, o objetivo da presente dissertação é desenvolver uma metodologia que permita assegurar a correta implementação da abordagem GRC. O desenvolvimento da metodologia em questão é feito através não só da utilização da metodologia FMEA ao longo de todo o processo de implementação e adaptação da abordagem GRC como também é complementado pela aplicação e configuração do *software* ServiceNow.

Tendo em conta a dimensão da empresa e consequente quantidade de dados de TI, a implementação da abordagem GRC é feita de forma faseada, sendo que, todo o processo é iniciado com a área de segurança em TI, presente na Digital Global Unit (DGU) da organização (*EDP*, 2021). A presente dissertação aborda, portanto, os riscos operacionais em TI na organização, sendo que, após esta primeira fase assente na área de segurança em TI, a organização pretende estender a abordagem de gestão do risco GRC para todas as restantes unidades de negócio do Grupo EDP. Desta forma, é garantida a centralização e acessibilidade de toda a informação relacionada a qualquer tipo de risco que a empresa enfrenta ou pode estar exposta, combatendo assim a limitação atual de segregação de dados por áreas e facilitando vários processos de auditoria no âmbito da gestão do risco.

Com o desenvolvimento da correta metodologia de adaptação da abordagem GRC ao estudo de caso pretende-se remediar a falta de interligação com os normativos da EDP, sendo esta outra limitação atual da gestão do risco da organização. A metodologia desenvolvida, que inclui a utilização simultânea da metodologia FMEA para atingir o objetivo de correta implementação da abordagem GRC, permite uma revisão estruturada das regras e boas práticas do grupo, descritas nos documentos normativos, e a sua associação a riscos existentes pela falta de *compliance* com as mesmas. Os riscos presentes nesta primeira fase de implementação, na área de segurança em TI, são monitorizados automaticamente e manualmente, devido à implementação do *software* ServiceNow, através de controlos baseados nas regras das diversas políticas e normas do Grupo.

A abordagem GRC garante, como primeiro *output*, uma visão realista do estado efetivo da empresa no que toca à gestão do risco em TI, e, futuramente, a mesma visão em termos globais do Grupo. Ao associar riscos com os ativos afetados pelos mesmos, controlos baseados

nas *standards* internacionais e responsáveis por ativos, por respostas a riscos e pela efetividade dos controlos, as limitações encontradas são assim mitigadas com a implementação desta abordagem.

1.4. Processo de Investigação

A equipa GRC, pertencente maioritariamente à DGU, pretende implementar a abordagem GRC com o objetivo de assegurar a segurança da informação, controlando todos os fatores de risco em conformidade com as políticas e normas da organização e monitorizando os respetivos controlos de forma centralizada e partilhada com todos os colaboradores. A DGU nasceu para ajudar o Grupo EDP a impulsionar a transformação para o novo mundo digital, sendo que a sua ocupação sustenta o desenvolvimento de novas ideias práticas que melhoram e otimizam os processos, simplificando a sua adoção tanto para os clientes como para os colaboradores.

O fluxograma representado na Figura 1.1 descreve o processo de investigação, desenvolvimento, implementação e análise da aplicação da abordagem GRC seguido para a realização da presente dissertação.

De forma a alcançar o sucesso da implementação da abordagem GRC no Grupo EDP e obter o retorno previsto sobre o investimento feito no projeto, foi definido o objetivo com a empresa, em particular com a equipa em trabalho direto com a implementação da abordagem em si, equipa GRC.

Para este efeito, foi primeiramente efetuada uma revisão da literatura sobre o tema geral de gestão de risco a partir do qual houve foco no tema de gestão do risco em TI. Investigou-se, ainda, as limitações existentes em tentativas de implementação de abordagens de gestão do risco em TI semelhantes e outras potenciais metodologias para tratar o tema. Após o agregar do conhecimento adquirido pelo processo de investigação, desenvolveu-se a metodologia descrita na presente dissertação. Esta foi ainda validada com os restantes membros da equipa GRC através de uma apresentação da mesma onde a estruturação do procedimento lógico foi demonstrado.

A metodologia de adaptação da abordagem GRC na área de gestão do risco em TI desenvolvida, apresentada e validada, inclui, principalmente e em relação à fase de recolha e correlação da informação regulamentar do Grupo, a utilização da metodologia FMEA acompanhada pelo *software* ServiceNow. O último suporta o processo de monitorização automática e manual dos controlos estabelecidos pela documentação regulamentar, facilitando, assim, os cálculos dos parâmetros de risco necessários à aplicação da metodologia FMEA.

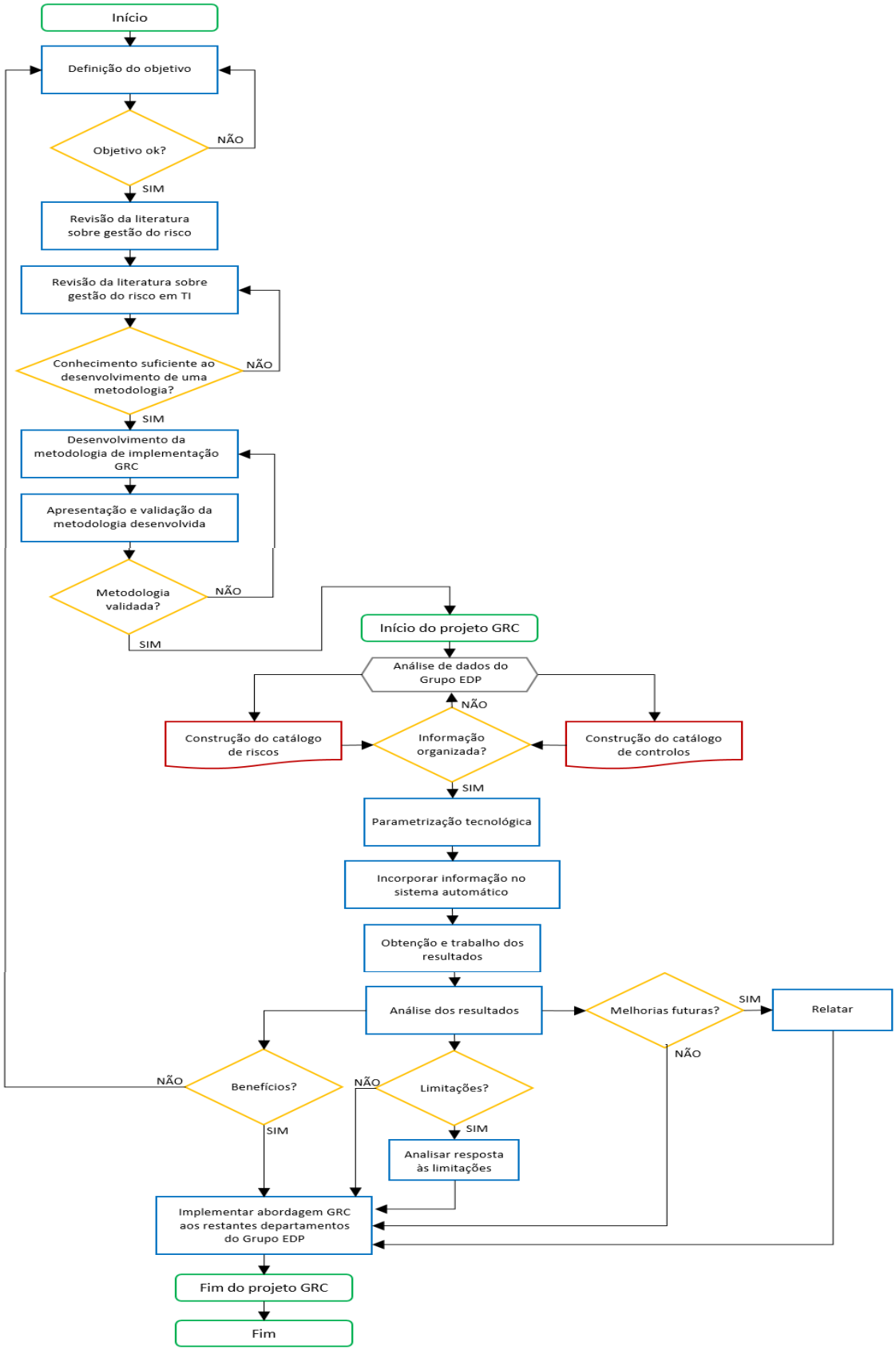


Figura 1.1 - Processo de desenvolvimento e implementação da abordagem GRC da presente dissertação

O processo inicial do projeto, de análise de dados, considera-se como, não só o mais demorado, como também crucial à eficácia e eficiência final da funcionalidade do projeto. Tal é devido, não só à imensidade de dados existentes, neste momento sem interligação entre si como é o caso dos controlos existentes em diversas áreas, por vezes repetidos, sem associação a riscos nem priorização dos mesmos, como também à existência de dados por documentar, como é exemplo dos riscos associados à não conformidade com a políticas e normas do Grupo EDP. Pretende-se, neste âmbito e recorrendo à metodologia FMEA, contruir um catálogo de riscos e controlos e a sua associação entre si e entre a legislação interna, a qual se baseia principalmente na ISO/IEC 27001:2013 mas também na COBIT e NIST. Este processo terá início com as áreas relativas à cibersegurança da organização, visto que a incorreta gestão das mesmas pode ter os efeitos mais drásticos.

Após a organização estratégica da informação, de forma a completar a metodologia FMEA, o projeto recorre à parametrização tecnológica do *software* ServiceNow, mais precisamente dos módulos de gestão do risco e conformidade. Neste processo são configurados os controlos necessários descendentes da documentação do Grupo assim como são inseridos os riscos identificados pelo uso da metodologia FMEA, identificação esta consequente do incumprimento das regras e princípios descritos nos normativos. Este *software* irá permitir uma *faster risk-based decision-making*, pois prioriza as atividades com base em pontuações de risco automatizadas. Desta forma prioritiza-se o trabalho nos riscos mais críticos, permitindo assim um maior desempenho da gestão do risco em TI da organização. Consequentemente, a gestão do risco efetua-se com atividades multifuncionais automatizadas, o que elimina interrupções de trabalho, e comunica os riscos de forma eficaz, pois *insights* em tempo real tornam os relatórios mais fáceis e rápidos, sendo que permite a realização de uma atualização constante dos riscos.

A automatização do processo de gestão do risco em TI permite a finalização do preenchimento da metodologia FMEA com dados concretos, reais e financeiramente pertinentes. Com isto, a fiabilidade dos resultados retiradas da utilização da metodologia FMEA é inquestionável pelo que a adaptação da abordagem GRC é bem sucessida. Os resultados são, seguidamente, analisados e destes são retiradas conclusões relativamente aos benefícios encontrados devido à metodologia de implementação concebida, limitações encontradas e o estudo de propostas de melhorias futuras.

1.5. Estrutura da Dissertação

Após a introdução, a presente dissertação segue-se com a revisão da literatura, a qual é abordada no Capítulo 2. É, neste capítulo, investigado o tema de gestão do risco, a sua relevância empresarial e ainda são descritos conceitos e definições associadas e identificados os vários tipos de risco que uma organização se pode encontrar exposta. Neste capítulo é dado, similarmente, ênfase à temática específica de gestão de risco em TI. É abordada não só a necessidade de um correto desempenho da gestão do risco em TI nos dias de hoje como também os processos, atividades e benefícios subjacentes à correta implementação deste tipo de gestão. Por fim são referidas as atuais limitações encontradas por vários autores nesta área, sendo

descritos e comparados vários modelos aplicacionais de gestão do risco em TI e identificados os seus pontos fracos e características de falta de *compliance* legislativa.

Segue-se o Capítulo 3, "Metodologias para Gestão do Risco em TI". No 3º Capítulo encontram-se referidas as metodologias selecionadas para a implementação da abordagem GRC assim como o conceito da abordagem em si e a seleção do respetivo processo aplicacional. Apresenta-se, assim, a explicação resumida do ciclo PDCA e da metodologia FMEA. Seguidamente é efetuado o estudo em detalhe da abordagem GRC proposta neste trabalho e clarificado o funcionamento do *software* escolhido para a implementação de tal abordagem. O capítulo inclui, portanto, a definição da abordagem GRC, onde são explorados os seus benefícios e ainda estudado o método correto para uma implementação bem-sucedida desta abordagem na gestão do risco em TI.

Ainda neste capítulo, como referido, introduz-se o tópico do ServiceNow. É importante referir que a utilização de um *software* de apoio é uma ferramenta crucial à correta implementação da abordagem GRC, como é justificado no Capítulo 3. É, então, primeiramente enunciado o motivo de escolha do *software* ServiceNow como ferramenta de apoio em comparação com outros inúmeros *softwares* disponíveis também para aplicação de gestão do risco em TI. Em seguida, efetua-se uma explicação detalhada do funcionamento do mesmo, em particular, dos módulos utilizados para efeitos de implementação em massa da abordagem GRC no Grupo EDP, sendo estes o módulo de risco e o módulo de *policy & compliance.*

No Capítulo 4 encontra-se a estruturação da implementação GRC. Esta inicia-se com o enquadramento prático desta implementação no Grupo EDP, onde são definidos os objetivos finais deste projeto, é feita uma análise da situação atual em termos de gestão do risco em TI na organização e definido o ponto de partida. Neste capítulo são ainda descritos os passos tomados para monitorizar o desenvolvimento da implementação da abordagem GRC, construído um *roadmap* referente aos níveis pelos quais este processo decorre em termos temporais e desenhado um plano de implementação ao nível das atividades necessárias à implementação deste serviço de gestão do risco em TI.

Em seguida, o Capítulo 4 inclui o detalhe e aplicação de cada fase do plano de implementação anteriormente estruturado, assim como a demostração das atividades nele assentes. As atividades referidas incluem o preenchimento da metodologia FMEA acompanhada pela configuração do *software* ServiceNow, mais uma vez faseadas segundo o plano.

Posteriormente, no Capítulo 5, são demonstrados os resultados da implementação da abordagem GRC na gestão do risco em TI no Grupo EDP. É, neste ponto, demonstrado e comprovado o cumprimento dos objetivos menciodados no planeamento do projeto e referidas as vantagens adquiridas pelo mesmo. Em particular, são referidos os benefícios relativos às competências que o *software* fornece à equipa de segurança da DGU, através da construção e atualização automática de *dashboards* informativos sobre o estado atual da organização nas diferentes frentes de interesse.

A presente dissertação finaliza com o Capítulo 6, "Conclusões". Este último capítulo apresenta estruturadamente as vantagens adquiridas no Grupo EDP devido à metodologia desenvolvida com o fim de uma bem-sucedida adaptação da abordagem GRC. Tais vantagens são confirmadas através, não só dos resultados obtidos após a implementação do projeto,

como também através dos contributos deixados à organização. Acrescenta-se, ainda, a proposta de algumas sugestões futuras cujo objetivo assenta na agilização e aumento de eficiência do processo desenvolvido nesta metodologia de implementação de gestão do risco em TI.

2. GESTÃO DO RISCO NAS TECNOLOGIAS DA INFORMAÇÃO

2.1. Gestão do Risco

O processo de gestão do risco tem sido do interesse de muitos investigadores. Apesar dos estudos alargados neste domínio, os resultados das aplicações práticas dos métodos propostos não correspondem às expectativas dos gestores empresariais (Aven, 2019). Os acontecimentos incertos, ambíguos e inesperados diminuem a previsibilidade de atingir objetivos de negócio e aumentaram a importância de uma organização fiável que é altamente resistente a eventos internos e externos indesejáveis. Os conceitos de risco e resiliência definem-se em várias disciplinas, incluindo ecologia, psicologia, social, económica, financeira e organizacional. Nesta dissertação, considera-se a gestão do risco organizacional (Soufi et al., 2021).

Todas as organizações estão expostas a vários riscos, por exemplo, ciberataques e perturbações causadas por desastres naturais (Torabi et al., 2016). O relatório Global Risks 2015 do Fórum Económico Mundial (GlobalRisks, 2015) afirma que os riscos ameaçam as vidas humanas e as atividades das organizações. As organizações são expostas a uma série de riscos que podem perturbar as suas atividades e causar muitos danos. Por exemplo, um incêndio numa fábrica de fornecedores causou perdas de 400 milhões de dólares para a Ericsson em 2000 (Norrman e Jansson, 2004). Por consequinte, os riscos devem ser geridos regularmente para evitar a perda de recursos e ativos. A elevada taxa de incidentes disruptivos, como os naturais ou tecnológicos, que ocorrem em todo o mundo, incentiva as organizações a conceber e implementar o seu próprio sistema de gestão de continuidade de negócio personalizado de forma a estarem preparadas para lidar com qualquer possível perturbação (Sahebjamnia et al., 2015). No entanto, a gestão de continuidade de negócios requer um quadro abrangente de Risk Assessment (RA) através do qual aqueles riscos que ameaçam as atividades das organizações possam ser identificados, analisados, avaliados e respondidos. Um quadro adequado de RA ajuda as organizações a fazer planos de contingência para parar de perder recursos no rescaldo de uma ocorrência de risco (Torabi et al., 2016).

Sendo que os processos e rotinas organizacionais estão cada vez mais dependentes de recursos, tanto humanos como naturais ou tecnológicos, interrupções e paragens devido a ataques, desastres ou erros no sistema, causam diversos riscos às organizações. A gestão do

risco diz respeito ao conjunto de métodos adotados para alcançar um equilíbrio entre os riscos e os custos das operações. A gestão do risco baseia-se, assim, na incerteza, o que significa que existe a capacidade de caracterizar a frequência sobre a relação de magnitude das perturbações com uma distribuição de probabilidades. Isto só é possível em caso de existência de dados históricos suficientes, assumindo que os processos se comportarão de forma semelhante ao passado (Soufi et al., 2021).

O conjunto de processos ou métodos de gestão do risco pretendem, primeiramente, identificar o risco para a empresa apresentado pela existência de ameaças internas e externas que estão sujeitas a ocorrer devido a vulnerabilidades internas ou falhas (Barafort et al., 2018). Sendo que, a identificação do risco, é vista como um processo crucial para prevenir eventos com consequências indesejadas relacionadas com ações que podem causar uma exposição vulnerável da organização (Sahebjamnia et al., 2015).

Em seguida, é feita uma avaliação do impacto efetivo, em caso de concretização dos riscos identificados, na empresa. O impacto pode ser descrito não só de forma subjetiva, onde são apresentados critérios como "alto impacto" ou "baixo impacto", como também de forma objetiva. Nesta última são apresentados critérios específicos como critérios financeiros, cuja abordagem pode ter em conta o preço de substituição de um servidor, o preço de reconstrução do *data center* da empresa, ou o preço de resposta a uma ação judicial ou processo legal (Fraser et al., 2021).

Após a avaliação dos riscos é necessário priorizar o tratamento dos mesmos de acordo com o impacto e a probabilidade de um risco ocorrer. É nesta fase de gestão do risco que a probabilidade de ocorrência deve ser atendida, uma vez que a variável de impacto não representa, na totalidade, a real dimensão do risco, sendo que, por exemplo, existem riscos de alto impacto negativo cuja probabilidade é rara. Considera-se, assim, essencial que o tratamento dos riscos seja priorizado de forma a dar resposta aos possíveis efeitos mais prováveis e significativos em primeiro lugar (Laine et al., 2021).

Também a avaliação da probabilidade de ocorrência de um risco pode ser quantificável ou qualificável. Podem ser, então, apresentados critérios de seleção deste fator tendo em conta as probabilidades de um risco específico ser tornado real. Tais critérios, em concordância com os níveis de impacto, podem ser avaliados desde "muito provável" a "pouco provável" ou até mesmo "raro", sendo que estes devem ter por base espectros específicos de forma a evitar uma avaliação não uniforme por parte das equipas de gestão do risco. Espectros estes relacionados com critérios temporais como a probabilidade de ocorrência do risco em 1, 5, 10 ou mais anos, por exemplo, tais definições temporais devem ser decididas tendo em conta os históricos e dados da empresa em si (Fikri et al., 2019).

O passo seguinte assenta na resposta ao risco. São consideradas quatro abordagens de resposta ao risco, sendo estas (Laine et al., 2021):

Evitar – Remover a vulnerabilidade, ou quando possível a ameaça, envolvida no risco. Para tal são aplicados controlos de forma a eliminar as vulnerabilidades internas existentes. Existe foco na remoção de vulnerabilidades visto que ameaças, no caso de riscos em TI, como modificações de *hardware* ou *software* sem autorização, falhas de *hardware*, *software*, *mídia* ou

serviços de comunicação ou modificação acidental de dados (edição, remoção ou inclusão), normalmente, não podem ser controladas.

Mitigar – Reduzir o impacto negativo ou a probabilidade de ocorrência de um risco através da implementação de controlos cuja finalidade inclui uma das duas reduções enunciadas, redução do impacto ou da probabilidade. Os controlos de tratamento de risco, que evitam ameaças de explorar vulnerabilidades presentes, têm, por norma, efeito em apenas um dos critérios, como resultado, são criados inúmeros e diversos controlos com o fim de mitigar os riscos respetivos a uma organização, variáveis com as especificações de cada empresa.

Transferir - Delegar toda ou parte da responsabilidade para um terceiro mitigando, assim, a responsabilidade da organização relativa a um risco. Um exemplo desta estratégia de tratamento do risco é a aquisição, por parte de uma organização, de seguros.

Aceitar - Reter algumas ou todas as consequências potenciais ou reais de um risco. Tal decisão é feita através de uma análise do custo-benefício entre os critérios de impacto e probabilidade que o risco representa e as consequências efetivas do mesmo ocorrer perante os custos de tratamento do risco, sejam estes através das abordagens enumeradas, evitar, mitigar ou transferir. Neste caso podem ser postos em prática planos para lidar com o risco após este ter efeito real na organização de forma a prever reações e atividades de controlo dos efeitos.

Após percorrida a etapa de tratamento dos riscos identificados e avaliados, segue-se a monitorização dos mesmos. Esta é, não só uma etapa de acompanhamento de riscos, como também o momento de reconhecimento de riscos novos, de observação da eficiência dos procedimentos estabelecidos e de implantação das medidas corretivas necessárias. Para o sucesso desta tarefa é importante referir a relevância da qualidade e tipo de ferramentas que recolhem informação relacionada com as ameaças assim como a sua interação com os indivíduos capacitados a esta tarefa (Aven, 2012; Aven e Krohn, 2014; Landquist et al., 2013).

A monitorização, para além de proteger a empresa contra possíveis ataques e ameaças, inclui outras vantagens como o fortalecimento das atitudes aplicadas em resposta aos riscos em si, sendo assim adicionado um carácter impessoal e objetivo às ações necessárias. Este processo de monitorização traz, ainda, benefícios como a redução de prejuízos organizacionais pois uma estratégia de monitorização bem estabelecida permite reduzir surpresas e, por consequentemente, custos e prejuízos associados. Permite ainda identificar novas oportunidades devido ao conhecimento atualizado de toda a informação presente na organização e otimizar o capital da mesma, pois é possível avaliar as necessidades e melhorar alocações de capital (Laine et al., 2021; Landquist et al., 2013).

2.1.1. Conceitos e Definições

Ameaça - Normalmente não podem ser controladas

Entende-se como ameaça, um evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso. As ameaças, normalmente, surgem da existência de

falhas não tratadas na segurança de uma organização. A ameaça é apresentada como a possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente, ou propositadamente, uma vulnerabilidade específica (Gewald e Dibbern, 2009; Perçin, 2008; Shi, 2007).

Vulnerabilidades Internas – Podem ser tratadas

Falha ou fraqueza de procedimento, *design*, implementação, ou controlos internos de um sistema que possa ser acidentalmente ou propositadamente explorada, que pode resultar, por exemplo, de uma violação da política de segurança do sistema (Zhang et al., 2018).

As vulnerabilidades não se relacionam apenas a fatores tecnológicos pelo que, estas podem estar associadas ao próprio comportamento dos usuários destes sistemas dentro de uma empresa, a fatores sociais diversos e a políticas de autorização ou autenticação do controlo de acessos.

Em TI, a vulnerabilidade é uma fraqueza que permite a um possível atacante a recolha de informação de um sistema tecnológico. Para esta ocorrer é necessário que exista a interseção de três elementos, sendo estes a existência de suscetibilidades ou falhas no sistema, a possibilidade de acesso do atacante à falha e a capacidade do atacante explorar a mesma (Kremljak e Kafol, 2014).

Controlos Internos – Podem ser controlados

Procedimento de controlo, ou seja, as políticas e procedimentos de monitorização que asseguram o cumprimento e garantem a execução das diretivas de gestão e segurança. Estes resultam da análise de conformidade com a legislação e políticas internamente estabelecidas. Permitem, assim, obter uma visão geral e específica da adequação da organização às normas e boas práticas recomendadas e obrigatórias.

Como parte da monitorização da performance legal de uma organização, os controlos internos testam continuamente a *compliance* da empresa. Sendo assim, uma empresa *compliante* é uma empresa apta a manter práticos os requisitos exigidos para o correto funcionamento da mesma. Tal é feito através da implementação, monitorização e auditoria dos controlos, garantindo e comprovando assim a sua adequação a estes (Fazlida, 2015).

Risco Externos e/ou Internos – Podem ser tratados

O risco encontra-se quando da ocorrência de qualquer evento que possa causar impacto negativo na capacidade de uma empresa. O risco pode ser definido como a combinação da probabilidade de um evento e as suas consequências.

Em todos os tipos de empreendimentos, existe o potencial de eventos e consequências que constituem oportunidades de benefício (positivo) ou ameaças ao sucesso (desvantagem). Para os sistemas é muito importante reconhecer diferentes tipos de riscos e avaliá-los (Kremljak e Kafol, 2014).

2.1.2. Tipos de Risco

Todos os riscos mencionados abaixo podem conduzir à redução, ou até mesmo perda, de valores para a empresa.

Risco Estratégico - Este é associado aos riscos que podem afetar a direção estratégica e a sobrevivência da organização. Os fatores que entram nesta categoria incluem os riscos macroeconómicos criados pelas políticas fiscais dos governos central e federal, bem como os impactos de tecnologias disruptivas, como a Internet. Estes riscos estão também associados a más decisões de negócios e definição de direção e são, ainda, extendidos a fusões e aquisições. É notório o fracasso de fusões e aquisições, sendo que os benefícios esperados das mesmas passam regularmente despercebidos. Considerando a quantidade de dinheiro investido em tais empreendimentos, o próprio facto de tantos fracassarem sugere uma gestão de risco deficiente (Garvey, 2008).

Risco Comercial/Financeiro - Cobre os riscos que podem afetar o negócio em termos de viabilidade financeira no geral. Inclui os riscos associados ao mercado em que a organização atua, ou seja, risco de mercado. Acrescenta-se os riscos referentes à capacidade de financiar o crescimento por meio de empréstimos, isto é, risco de crédito. São normalmente riscos bem compreendidos, com um grande número de instrumentos financeiros e técnicas disponíveis para o gestor de risco (Campbell, John, 2001).

Risco de Programa e Projeto - Assenta no risco de uma iniciativa de mudança significativa falhar ou de os benefícios esperados pela mesma não se concretizarem. Com um uso cada vez maior de projetos e programas para impulsionar a mudança dentro das organizações, este tipo de risco costuma estar intimamente associado ao risco estratégico, pois, a falha pode ter impactos consideráveis na organização. Além disso, com a crescente complexidade das organizações, a gestão do risco de programa e projeto tem-se tornado uma habilidade essencial (Balke, 2014).

Risco Operacional - Esta é uma categoria de risco abrangente que inclui a falha de qualquer aspeto das operações de uma empresa. Inclui falhas de gestão, falhas de sistemas e *software*, erro humano, ineficiências de processo e falhas de procedimento. Embora relativamente recente, é reconhecido como uma parte importante de uma estrutura geral de gestão do risco.

Os riscos em TI são considerados riscos operacionais, relacionados ao uso, operação e influência da tecnologia da informação dentro de uma organização, envolvendo, assim, problemas como a interrupção dos sistemas, problemas de segurança e outras complicações. Podem ocorrer riscos de uso de benefícios ou valores de TI, sendo estes os riscos relacionados com a perda de oportunidades do uso da TI como uma forma de melhoria na eficiência dos processos empresariais, ou até mesmo sob a forma da criação de novas iniciativas de negócios (Bristow et al., 2013).

Existem ainda outras categorias de risco, sendo estas mais generalizadas e de alto nível. Exemplos relativos aos riscos destas categorias encontram-se em seguida.

Risco Técnico - Problemas geotécnicos inesperados, solicitações de mudança devido a erros, suposições imprecisas sobre questões técnicas na fase de planeamento, análise do local de resíduos perigosos incompleta ou com erros, necessidade de exceções aos padrões, etc (Aven, 2012; Kremljak e Kafol, 2014).

Riscos Externos - Proprietários de terras que não desejam vendê-las, custo, tempo e objetivos de qualidade inconsistentes, comunidades locais apresentam objeções, mudanças de financiamento para o ano fiscal, alterações políticas, *stakeholders* solicitam modificações tardias, novos *stakeholders* surgem e exigem novos trabalhos ou apelam por necessidades adicionais de serviços comerciais, ameaças de processos judiciais, etc (Kremljak e Kafol, 2014).

Riscos Ambientais - Licenças ou ações de agências desatualizadas, novas informações necessárias para licenças, mudanças nas regulamentações ambientais, mudanças na regulamentação da qualidade da água, falta de pessoal especializado (biologia, antropologia, arqueologia, etc. .) sítio histórico, espécies em vias de extinção, polémicas ambientais inesperadas, etc (Crovini et al., 2021; Kremljak e Kafol, 2014).

Riscos Organizacionais - Equipa designada inexperiente, perda da equipa crítica no ponto crucial do projeto, tempo insuficiente de planeamento, carga de trabalho imprevista do gestor de projeto, atrasos causados por documentação interna na obtenção de aprovações, unidades funcionais indisponíveis, falta de compreensão de procedimentos de financiamento interno complexos, mudança de prioridades no programa existente, etc (Aven, 2013).

2.2. Gestão do Risco em TI

A TI está mais do que nunca presente, para empresas, para redes de negócio, para soluções de *cloud computing*, *internet of things*, dispositivos conectados e móveis e muitas mais aplicações na Internet. A TI tornou-se omnipresente e essencial para qualquer negócio. Devido à sua natureza indispensável, a gestão dos riscos tornou-se também vital. Em todos os domínios, as atividades de gestão dos riscos devem estar sob controlo. Pode ser para fins dedicados à gestão do risco ou numa perspetiva mais ampla em sistemas de gestão, sendo que, um sistema de gestão é definido pela ISO/IEC 27001:2013 como o conjunto de elementos interrelacionados de uma organização, política, objetivos, processos e a forma de alcançar esses objetivos. Ainda é acrescentado a esta definição que um sistema de gestão pode abordar uma única disciplina ou várias disciplinas. Nos *settings* de TI, muitas atividades estão fortemente relacionadas com a gestão dos riscos, os principais domínios consideram-se a gestão de projetos, segurança da informação e gestão de serviços de TI. A ISO/IEC 27001:2013 define o risco como o efeito de não-fiscalização sobre os objetivos, e uma nota para esta definição refere que os objetivos podem ter aspetos diferentes (tais como objetivos financeiros, de saúde e de segurança e ambientais) e podem ser aplicados a diferentes níveis (como estratégicos, organizativos, projetos, produtos e processos) (Barafort et al., 2017).

O crescente aparecimento de ameaças à segurança da informação exige a integração da gestão do risco em TI na gestão corporativo da organização. A exposição ao risco de segurança da informação devido à atual digitalização cria uma necessidade de tratar a segurança da informação como uma prioridade tão elevada como outra área crítica de governação corporativa por conselhos de administração e gestão executiva (Fazlida, 2015).

De todas as novas ameaças existentes deve ser dada prioridade à continuidade do negócio e recuperação de desastres, riscos cibernéticos e ameaças cibernéticas, fuga de dados e prevenção de perda de dados, transformação da segurança da informação e monitorização da

conformidade (Ernst e Young, 2014). O objetivo da segurança da informação é proteger e preservar a confidencialidade, integridade e disponibilidade de informação. Pode igualmente implicar a proteção e preservação da autenticidade e fiabilidade da informação e a garantia de que as entidades possam ser responsabilizadas quando da materialização dos potenciais riscos em TI.

A gestão do risco em TI é, portanto, um processo complexo que envolve todas as áreas de uma empresa, permitindo um trabalho conjunto com o fim de proteger informação que cause qualquer tipo de vulnerabilidade. Estão, assim, envolvidos nesta área de gestão, equipas como o Comité de Auditoria, equipa de gestão de TI, equipa de segurança, onde é feita a avaliação e identificação de risco no negócio, e todos os níveis de gestão, de forma a auxiliar a equipa de segurança no sucesso dos seus processos de gestão do risco (Crovini et al., 2021; Sahebjamnia et al., 2015).

As principais atividades realizadas em gestão do risco em TI baseiam-se na determinação dos níveis de risco que a organização está disposta a aceitar e no desenvolvimento de políticas de gestão dos riscos, através de estruturas, catálogos e demonstrações de risco. Acrescenta-se ainda atividades de desenvolvimento de procedimentos de avaliação e resposta ao risco, implementação de controlos de redução da exposição ao risco e a sua respetiva periocidade e a determinação de formas de medição, definição de indicadores, e medidas de melhoria contínua de acordo com os resultados atingidos (Barafort et al., 2018).

A ISO 31000 (2018, p.1) define o risco como "efeito da incerteza nos objetivos". Por consequinte, o Risco de Segurança da Informação (ISR) pode ser definido pela ISO 31000 como uma combinação de dois fatores: probabilidade e consequências. Coloca, assim, duas questões básicas:

- Qual é a probabilidade de um determinado evento de segurança da informação ocorrer no futuro?
- Que consequências este evento produziria ou que impacto teria se realmente ocorresse? (Fazlida, 2015).

A gestão da segurança da informação torna-se, assim, uma atividade muito focada, com condutores de valor específico, incluindo integridade da informação, continuidade de serviços e proteção de ativos de informação. A gestão da segurança da informação pretende o estabelecimento e manutenção do ambiente de controlo para gerir os riscos relacionados com os processos e sistemas de apoio informático que não fazem parte da auditoria. Garante ainda que os processos de governação foram devidamente estabelecidos e funcionam, assim como a operação de segurança, o desempenho diário das atividades administrativas de segurança, e a engenharia de novas TI ou processos para cumprir objetivos de segurança. Esta área de gestão acarreta, além do descrito, a responsabilidade de proteger o valor dos acionistas. Esta responsabilidade aplica-se tão rigorosamente aos ativos de informação valorizados como a qualquer outro ativo. O Conselho de Administração deve reconhecer que assegurar a informação não é apenas um investimento, mas sim essencial para a sobrevivência e criação de vantagens competitivas (Klein Jr. e Reilley, 2021).

A implementação de uma correta e bem-sucedida gestão do risco em TI requer envolvimento e empenho de vários departamentos dentro das organizações com adesão à política de

segurança da informação corporativa e referência aos códigos de conduta de segurança da informação. A ISO/IEC 27001:2013 é apontada como o principal quadro para a segurança da informação, enquanto que o COBIT é internacionalmente conhecido e utilizado, este é também criticado por ter limitação na área da segurança da informação (Everett, 2011; ISO 27001:2013, p. 27).

A gestão eficiente da segurança da informação é alcançada quando a gestão executiva coloca especial atenção em questões relativas ao risco da segurança da informação, em vez de a tratarem como questões tecnológicas sob responsabilidades dos gestores técnicos. As medidas de segurança da informação devem ser claramente comunicadas da administração de topo para os colaboradores pois estes fazem parte do processo de formulação das políticas de segurança da informação, evitando, assim, uma possível rejeição da implementação das mesmas. Por último, todas as partes interessadas devem estar conscientes do valor acrescentado oferecido pela implementação da gestão da segurança da informação, este último fator resulta num maior investimento no controlo da segurança da informação (Fazlida, 2015; O'Leary, 1990).

O mais importante na superação das questões relacionadas com o risco é que as organizações devem prestar atenção à construção, melhoria e gestão do nível de confiança antes, durante e após a ocorrência de um incidente. Sendo a gestão do risco para a segurança da informação um dos focos da atual gestão do risco, a ISO 27005:2011[1] é uma norma amplamente utilizado pelas organizações na implementação da gestão mencionada (Fikri et al., 2019).

Na fase de implementação, a ISO 27005:2011 pode ser combinada com outras normas ou orientações para satisfazer as necessidades organizacionais relativas à gestão dos riscos de segurança da informação. Espera-se que outras normas ou orientações apoiem o processo de gestão dos riscos com base na segurança da informação. A revisão NIST SP 800-30 1 pode ser utilizada como complemento ao processo de avaliação de riscos e pode ser aplicada ao quadro de gestão do risco ISO 27005:2011 (Everett, 2011, p. 2; ISO, 2021; Meriah e Arfa Rabai, 2019).

Uma orientação adequada para a avaliação dos riscos é a revisão 1 da Publicação Especial NIST 800-30. Esta revisão fornece orientações de avaliação de riscos para sistemas de informação de organização e governamentais e como complemento da NIST SP 800-39. As normas de segurança e outras orientações apoiam a abordagem da revisão de risco NIST SP 800-30, a fim de gerir os riscos de segurança da informação. As etapas desta orientação incluem a identificação da fonte de ameaça, a identificação de ameaças de eventos, a identificação da vulnerabilidade, a determinação da probabilidade, a determinação do impacto e a determinação do nível de risco (Fikri et al., 2019).

2.2.1. Necessidade da Correta Abordagem de Gestão do Risco em TI

A *cloud computing* é um dos tópicos críticos no domínio de TI do século XXI. Após anos de discussão rigorosa e entusiasta, *cloud computing* evoluiu gradualmente desde a introdução

[1] A ISO 27005:2011 define as melhores práticas de gestão do risco que são adaptadas principalmente para "information security risk management", com ênfase especial na conformidade com os requisitos do *Information Security Management System* (ISMS), conforme exigido pela ISO/IEC 27001.

do conceito ao desenvolvimento de aplicações e, consequentemente, tornou-se um dos campos promissores em que as empresas e a indústria de TI começam a investir massivamente. As características desta tecnologia incluem uma escalabilidade dinâmica, onde a digitalização desempenha um papel bastante relevante (S.-H. Li et al., 2015). Como efeito, as empresas começaram a perceber a importância da digitalização e a investir fortemente na sua implementação (Q. Li et al., 2010).

Como definição, tem-se que *cloud computing* é uma tecnologia de computação recentemente desenvolvida que utiliza recursos de digitalização para fornecer serviços de TI através da tecnologia da Internet (Chou, 2015a). Ainda, Marston (2011) define a tecnologia como "um modelo de serviço de tecnologia da informação onde os serviços de computação, ou seja, *hardware* e *software,* são entregues a pedido aos clientes através de uma rede, em forma de *self-service*, independente do dispositivo e da localização".

O Instituto Nacional de Normalização e Tecnologia (NIST) também definiu *cloud computing* como "um modelo para permitir o acesso conveniente, a pedido de rede, a um conjunto partilhado de recursos configuráveis de computação, por exemplo, redes, servidores, armazenamento, aplicações e serviços, que podem ser rapidamente alocados e libertados com o mínimo esforço de gestão ou interação de prestadores de serviços" (CPA, 2009).

Entre os benefícios potenciais, a digitalização permite centralizar e integrar os recursos de TI. O armazenamento de dados centralizado facilita o *back-up*, impede a redundância e melhora o controlo de qualquer tipo de dados. Facilita, igualmente, uma melhor conformidade com as regulamentações e a gestão das TI. Em segundo lugar, a digitalização ajuda a reduzir o número de servidores e, ao fazê-lo, tende a reduzir o uso de instalações de potência e arrefecimento. O número reduzido de servidores e uso de potência pode não só aliviar a pressão da eficiência na gestão das TI, mas também estar em conformidade com a tendência generalizada para a energia global (Li et al., 2015).

Tal área de computação recentemente desenvolvida é utilizada por várias organizações para vários fins. As organizações que investem na prática de *cloud computing* pretendem obter os possíveis benefícios por esta gerada. Enumeram-se benefícios como a poupança nos custos, a melhoria da eficiência, o reforço da agilidade, a flexibilidade, a expansão de escalabilidade e a sustentabilidade ambiental. *Cloud computing* ganha, assim, popularidade, uma vez que muda a indústria de TI, partilhando recursos através da ideia de digitalização. No entanto, uma das principais preocupações existentes com esta nova tecnologia é o seu ambiente virtualizado, que por sua vez, implica uma cuidada gestão das TI (Chou, 2015b).

É possível ainda comparar o funcionamento do modelo operacional de *outsourcing* de sistemas de informação ao *cloud computing*, pois, ambas as práticas demonstraram a capacidade de utilização de recursos, digitalização, escalabilidade e agilidade. A similaridade entre as duas práticas encontra-se no uso de *hardware*, *software*, infraestrutura ou capacidades de armazenamento de fornecedores externos para processos internos de Tecnologias de Informação e Comunicação (TIC) (Chou, 2015b). O *outsourcing* de sistemas de informação é uma prática importante no funcionamento do negócio, pretende dar resposta às necessidades de uma empresa sendo que, *outsourcing* do processo de negócios integra a gestão corporativa como estratégia organizacional (Chou, 2007).

Embora esta prática cada vez mais aplicada empresarialmente traga uma série de benefícios, tais como a redução dos custos operacionais, o acesso a novas tecnologias e tecnologias atualizadas, a partilha de recursos e riscos, entre outros, existem riscos envolvidos neste processo. Uma vez que os projetos de *outsourcing* de sistemas de informação envolvem organizações externas para a construção e manutenção de *software*, a capacidade de ocorrências de risco é relativamente maior do que a dos projetos *inhouse.* Os riscos de subcontratação de sistemas de informação afetam a qualidade do serviço aos clientes de forma direta e indireta. Riscos estes que podem incluir custos de transição e gestão não previstos, alterações contratuais dispendiosas, difamação de serviços, perda de competências organizativas, aumento dos custos, e custos de serviços (O'Leary, 1990).

Como a prática de *outsourcing*, também *cloud computing* apresenta possíveis riscos quando da sua integração. O risco de segurança é a preocupação mais significativa para o *cloud computing* uma vez que os dados da organização são armazenados numa área remota, processo este que levanta preocupações de privacidade, confidencialidade, controlo de acessos e a própria gestão de ativos (Chou, 2015b). (CPA, 2009), na sua revisão das normas de avaliação da segurança da digitalização, argumentou ainda que os riscos de segurança da digitalização compreendem os riscos dos dados transportados de um ambiente de servidor físico, aqueles que se desdobram com digitalização devido à rapidez e facilidade de implementação de fontes informáticas e os riscos exclusivos das ferramentas de digitalização.

Existem, portanto, muitas questões a resolver no que diz respeito à implementação ou adoção de digitalização. Uma das questões mais importantes pode ser as inquietações de segurança no que diz respeito às máquinas virtuais e aos ambientes virtualizados. Estudos recentes revelam aspetos desafiantes e benéficos da digitalização em matéria de segurança da informação (Christodorescu et al., 2009; CPA, 2009; Steven J. Vaughan-Nichols, 2021). Além disso, sugere-se que as medidas de segurança sejam aplicadas e adotadas à medida que as empresas se movem para a digitalização. No entanto, a implementação de medidas de segurança requer regulamentações específicas para apoiar, auditar e monitorizar. A ISO/IEC 27001:2013 é atualmente uma das normas de segurança da informação mais aceites e, por consequinte, altamente adequada para servir de orientação para a implementação e avaliação de medidas de segurança da informação diferentes dos sistemas virtualizados (Li et al., 2015).

A série de normas ISO/IEC 27000 publicada pela International Standard Organization (ISO) e pela International Electrotechnical Comnion (IEC) são as normas dedicadas à segurança da informação. Especificamente, a ISO/IEC 27001:2013, focada nas tecnologias da informação, técnicas de segurança, sistemas de gestão da segurança da informação e respetivos requisitos, fornece a definição e os requisitos importantes de um sistema de gestão da segurança da informação (Li et al., 2015). Acrescenta-se ainda que, em muitas organizações de TI, os sistemas de gestão são mandatados pelo mercado em termos de certificações tais como a ISO/IEC 27001:2013 para a gestão da segurança da informação (Barafort et al., 2018).

Hoje em dia, a gestão do risco é, assim, um desafio fundamental para a maioria das organizações. As organizações que desejam melhorar a gestão dos riscos enfrentam o problema de escolher e selecionar a abordagem certa, orientada para os seus desafios comerciais e posicionamento no mercado (Barafort et al., 2018). Tal é devido ao facto de que as empresas

podem estar expostas a ataques devido a má gestão ou medidas de segurança insuficientes ou desadequadas (Li et al., 2015). (Barafort et al., 2018) teorizaram que uma abordagem integrada de gestão do risco para as organizações beneficiará as mesmas, baseando-se em normas ISO que apresentam um consenso internacional. A suposição dos autores é apoiada pela procura de mercado para normas ISO 9001, ISO/IEC 27001:2013 e ISO 20000-1, as mais utilizadas para certificação de sistemas de gestão.

2.2.2. Relevância da Implementação da ISO/IEC 27001:2013

As autoridades públicas não são as únicas com cada vez mais exigências em termos de conformidade. Grandes empresas do sector privado são igualmente encorajadas a manter regulamentos ou, pelo menos, a encorajar fornecedores e parceiros a considerar tomar este tipo de ação. Esta tendência é devida, em grande parte, à necessidade, por parte das empresas, da normalização de processos de licitação e aquisição. Tal ocorre com o objetivo de otimizar procedimentos repetitivos como o preenchimento de questionários pormenorizados (Aven e Krohn, 2014; Mesquida et al., 2014).

Para as organizações que entendem o valor iminente da conformidade, uma das considerações mais relevantes é a compreensão do risco a que se encontra sujeita a informação. Estabelecer quais os riscos do negócio que a exposição das TI podem afetar e trabalhar como atenuá-los para um nível e custo aceitáveis é crucial. Igualmente crítico é a compreensão, por parte das organizações, que a gestão da segurança da informação ou a gestão do risco em TI deve ser tratado como uma questão de governação empresarial e, como tal, deve seguir normativos de gestão de processos, políticas e pessoas. Como resultado, profissionais de segurança da informação encarregados de implementar padrões regulamentares, normas e leis devem reportar ao conselho de administração. Devem, ainda, garantir que o risco de informação é adicionado para o registo de risco corporativo, que hoje tende a incluir apenas risco de negócios operacionais, financeiros, de saúde e de segurança (Everett, 2011).

O elemento mais útil da conformidade programa encontra-se, exatamente, na avaliação minuciosa de risco. Uma vez que 60-70% dos 133 controlos na ISO/IEC 27001:2013 são orientados para as TI, a conformidade com a mesma na identificação, análise, avaliação de risco da segurança da informação e na documentação e atualização dos resultados obtidos permite, às empresas, não só descobrir lacunas nos processos e atividades organizacionais de TI como também procedimentar medidas corretivas e reações a problemas já documentados (Everett, 2011; Fikri et al., 2019).

2.2.3. ISO/IEC 27001:2013

Em função dos objetivos estratégicos da organização, da vantagem competitiva no mercado e dos condicionalismos de regulação e de conformidade, as empresas de TI ou os departamentos de TI podem necessitar de certificados no que diz respeito aos requisitos dos sistemas de gestão, tais como a ISO/IEC 27001:2013 para a segurança da informação. Podem igualmente ter que integrar normas mais gerais relacionadas com as TI, como a ISO 9001 para o sistema de gestão da qualidade. Esta situação é cada vez mais frequente e exige integração e interoperabilidade para a poupança de custos, redução da complexidade, eficiência e eficácia.

Isto é particularmente verdade para a gestão dos riscos que é central nas organizações de TI com sistemas de gestão integrados e pensamento baseado no risco (Barafort et al., 2017).

A fim de satisfazer os constrangimentos de mercado que muitas empresas enfrentam atualmente e fornecer uma perspetiva ampla e neutra, é necessário implementar uma abordagem integrada de gestão dos riscos em TI baseada nas normas ISO visto os benefícios que a certificação nas mesmas proporciona. As normas internacionais representam, assim, o consenso internacional, proporcionam um acesso aberto aos domínios técnicos, bem como o posicionamento voluntário em direção a certificações, e contribuem para os benefícios das empresas. Os benefícios gerados são principalmente devidos à promoção da padronização (ISO 27001, 2013).

No domínio das TI, com a primeira publicação em 2005 das ISO 20000-1 e ISO/IEC 27001:2013, novas normas do sistema de gestão entraram em vigor internacionalmente, respetivamente para a gestão de serviços de TI. Entre os aspetos integrativos dos sistemas de gestão em TI, existem muitos trabalhos de investigação, direcionando a gestão dos riscos com aplicações em muitos domínios. Assim, a gestão do risco desempenha um papel importante e é omnipresente nos sistemas de gestão (Barafort et al., 2017; Klein Jr. e Reilley, 2021).

Do ponto de vista das normas ISO, a norma ISO 31000 sobre a gestão do risco é a principal referência, com uma visão holística sobre a gestão dos riscos. Além disso, em muitos domínios existem normas dedicadas de gestão dos riscos onde várias metodologias-alvo são citadas para implementação, no caso da gestão dos riscos de segurança da informação, onde se tem em conta riscos específicos de TI, é aplicada a ISO/IEC 27001:2013, que inclui riscos como os associados à tecnologia *cloud computing* (Chou, 2015b). Quando comparadas com as metodologias, estas pesquisas visam o "Como", e não se concentram no "O quê", que é abordado por processos e que não é prescritivo quando visto de uma perspetiva genérica (CPA, 2009; S.-H. Li et al., 2015).

A ISO/IEC 27001:2013 faz parte da família de normas ISO 27000 que tem como objetivo ajudar as organizações a manter o segredo dos ativos da informação. A ISO/IEC 27001:2013 é a norma mais conhecida nos requisitos de proscrição familiar para um sistema de gestão da segurança da informação. O sistema mencionado é uma abordagem sistemática da gestão de informações da empresa para que se mantenha segura. Pode ser aplicada às pequenas, médias e grandes empresas de qualquer sector. Inclui pessoas, processos e sistemas de TI aplicando um processo de gestão do risco (Barafort et al., 2017).

O processo de avaliação e tratamento do risco de segurança da informação na ISO/IEC 27001:2013 alinha-se com os princípios e orientações genéricas estabelecidos na ISO 31000:2018, bem como com o estabelecimento do contexto externo e interno da organização. A ISO/IEC 27001:2013 inclui "Requisitos para a avaliação e tratamento dos riscos de segurança da informação adaptados às necessidades da organização". Além disso o sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da formação através da aplicação de um processo de gestão dos riscos e dá confiança às partes interessadas de que os riscos são geridos adequadamente (ISO 27001, 2013).

Relativamente à liderança e compromissos a norma defende que "a gestão superior deve evidenciar os seus compromissos de planeamento, criação, implementação, funcionamento,

monitorização, revisão, manutenção e controlo dos seus sistemas e serviços, garantindo que os riscos são avaliados e geridos". Da mesma forma que na ISO 9001, quando se planeia o sistema de gestão da segurança da informação de acordo com a ISO/IEC 27001:2013, podemos aferir que "a organização determinará os riscos e oportunidades que devem ser abordados" e que "os objetivos de segurança da informação devem ter em conta a avaliação dos riscos e os resultados dos tratamentos de risco" (Everett, 2011; ISO, 2021).

Relativamente ao tratamento dos riscos a ISO/IEC 27001:2013 considera que "a organização deve avaliar os riscos de segurança da informação em intervalos previstos ou quando forem propostas ou ocorram alterações significativas. As organizações retêm informações documentadas sobre os resultados das avaliações de risco de segurança da informação". A ISO/IEC 27001:2013 também contém uma cláusula sobre como "aplicar o processo de avaliação do risco de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade de informação no âmbito do sistema de gestão da segurança da informação e identificar os investidores". A ISO/IEC 27001:2013 considera explicitamente como necessidade a análise dos riscos de segurança da informação, a avaliação das potenciais consequências que ocorreriam se os riscos identificados se concretizarem e a avaliação sobre a situação realista da ocorrência dos riscos identificados. Estabelece ainda que os riscos para a segurança da informação devem ser reavaliados de forma a "comparar os resultados da análise de risco com os critérios de risco e priorizando os riscos analisados para o tratamento de risco", sendo que "a organização deve conservar a informação documentada dos resultados do tratamento de risco de segurança da informação"(ISO 27001, 2013).

Relativamente à monitorização e revisão, esta deve ser uma parte planeada do processo de gestão dos riscos e envolver uma verificação regular ou uma vigilância consistente e constante. "A gestão de topo deve, ainda, rever o sistema de gestão da segurança da informação da organização em intervalos previstos, a fim de assegurar a sua contínua adequação e eficácia. A revisão da gestão deve excluir a apreciação dos resultados da avaliação dos riscos e do estatuto do plano de tratamento de riscos". De acordo com a norma, com base nos resultados de monitorização e revisão, devem ser tomadas decisões sobre a forma como o quadro de gestão dos riscos, a política e o plano podem ser melhorados (Barafort et al., 2017, 2018; ISO 27001).

A abordagem da estrutura utilizada na ISO/IEC 27001:2013, segue o processo de gestão da ISO 31000:2009, representada na Figura 2.1. Este processo de gestão facilita a integração das diferentes atividades específicas para o planeamento da gestão dos riscos, a execução de planos de tratamento de riscos, a monitorização da eficácia do processo de gestão dos riscos e a melhoria do quadro de gestão dos riscos aplicados (Barafort et al., 2017).

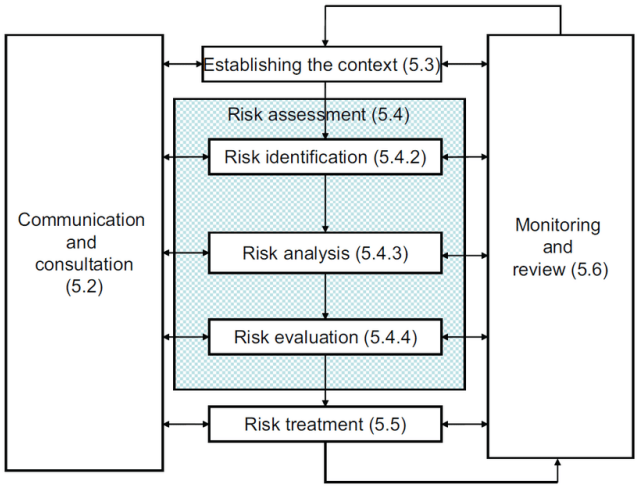


Figura 2.1 - ISO 31000:2009 (EN, 1st Edition – outdated, revised in 2018) (p. 22)

2.2.4. Limitações Atuais da Gestão do Risco em TI

A maioria das empresas adota normas de segurança da informação para gerir as suas questões relacionadas com as TI de forma a garantir um ambiente propício para o seu funcionamento. Apesar destas medidas, as violações de dados são evidentes e evoluem a partir de novas dimensões. Por exemplo, o *cloud computing* conduziu a novos riscos de segurança devido a alterações nas funções das organizações de clientes. Embora a segurança da informação da tecnologia *cloud computing* tenha muitas semelhanças com os serviços tradicionais de TI implantados numa empresa, vale a pena notar que introduz ameaças significativas que devem ser reavaliadas (Kaufmann, 2017; Ramalingam et al., 2018).

A gestão dos riscos é uma questão crucial na segurança da informação que se esforça por encontrar um equilíbrio entre os custos e as medidas de segurança. O problema subjacente é identificar e priorizar riscos potenciais de uma superfície de risco maciça. Investigadores sugerem que avaliações periódicas de risco associadas à monitorização contínua dos riscos em evolução podem diminuir as ameaças. Hoje em dia, as organizações reconhecem que várias tecnologias e processos heterogéneos que funcionam em silos conduzem inevitavelmente à ineficiência, ao aumento dos custos e à apresentação de fatores de risco mais elevados (Grey, 1995). A fim de ultrapassar estas limitações, os peritos em segurança da informação estão a concentrar-se no quadro abrangente e adaptativo baseado em políticas que abrange a solução TI-GRC (Hohan, 2015).

A segurança da informação centra-se em dimensões como gestão e tomada de decisão, avaliação de risco e conformidade com a segurança (Ramalingam et al., 2018). Estas três dimensões consolidam-se nos processos de Governação, Gestão do Riscos e Conformidade através dos quais a gestão identifica estrategicamente, analisa e, se necessário, responde adequadamente aos riscos que podem afetar negativamente a realização dos objetivos empresariais de uma organização (Kaufmann, 2017). A implementação do TI-GRC torna-se complexa e mo-

rosa devido à alteração do panorama das TI e às dificuldades na medição da eficiência e eficácia dos objetivos de controlo. A questão surge na utilização de ferramentas IT-GRC *off-the-shelf*. Estudos indicam que, devido à natureza das organizações e ao seu ambiente interno e fatores operacionais, certas ferramentas comerciais TI-GRC não fornecem soluções otimizadas (Hohan, 2015).

O sucesso da TI-GRC depende da sua sincronização dentro da organização. As funções TI-GRC devem ser associadas umas às outras de tal forma que cada uma complementa a outra. Por exemplo, os programas de gestão ajudam a conceber a estratégia de TI, avaliando os controlos necessários para o cumprimento da mesma. Da mesma forma, um programa de conformidade explora fatores de risco para justificar os controlos necessários. Finalmente, a gestão do risco avalia o risco com base na governação das TI e mecanismos de conformidade para normalizar o perfil de risco da organização. Da discussão acima, é evidente que o sucesso da implementação do TI-GRC depende da sua coordenação mútua. A adoção de um quadro de controlo comum para implementar um programa TI-GRC é necessária para alcançar tal sincronização. Uma grande variedade de normas e quadros de controlo de segurança de TI estão disponíveis para as organizações explorarem os seus benefícios. Sendo que, algumas normas, como a ISO/IEC 27001:2013, definem os controlos operacionais (Fikri et al., 2019; Fraser et al., 2021).

Ramalingam et al. (2018) recomenda que a organização escolha o padrão de controlo ou o quadro que pode implementar, medir e proporcionar um ambiente para explorar as novas oportunidades e ameaças com um custo aceitável que possa justificar o retorno do investimento.

Alcançar uma implementação bem-sucedida da segurança da informação com uma gestão optimizadamente equilibrada, a gestão e o cumprimento dos riscos é uma tarefa complexa, uma vez que existem vários desafios que devem ser abordados pelos decisores. Limitações encontradas até ao momento encontram-se listadas abaixo (Hunt, 2014):

- Os relatórios apresentados frequentemente pelos gestores de segurança não facilitam a tomada de decisões, uma vez que os valores numéricos obtidos por métodos qualitativos tendem a ocultar a sua natureza e não informam a influência e as causas reais;
- As técnicas de medição qualitativa são consideradas a prática base em muitas organizações que muitas vezes são baseadas em informações subjetivas, todavia, não são adequadas para medir a eficácia dos controlos. Além disso, os controlos e o reforço destes não são realistas;
- Uma vez que os riscos emergentes não são considerados de forma realista, as estratégias empresariais e os planos operacionais não se sincronizam, o que impossibilita a previsão da eficácia dos controlos de segurança;
- As métricas quantitativas derivadas das plataformas comerciais TI-GRC não refletem a situação real, uma vez que não adotam metodologias cientificamente comprovadas em contexto adequado e não indicam qualquer correlação que a torne imprópria para a tomada de decisões.

Uma métrica de segurança é um atributo que pode quantificar a eficácia das medidas de controlo de segurança de uma organização. Outro estudo refere, no entanto, que as empresas veem as métricas de segurança como uma das partes essenciais da avaliação da segurança

da informação, obter precisão nesta medição é considerado como um processo difícil (Ramalingam et al., 2018). Vários investigadores também argumentam que existem dificuldades na decisão sobre o que medir e como apresentá-la em toda a organização, de forma que seja significativa para a tomada de decisões estratégicas. Além disso, as métricas quantitativas muitas vezes não são colocadas em contexto adequado, tornando-as subutilizadas, mesmo alguns estudos simplesmente tentam medir as características mais fáceis, como uma série de falhas de *login*, no entanto, não correlacionam e estudam as interdependências entre os vários controlos, tornando assim ineficazes para a tomada de decisões. Outros investigadores argumentam que o questionário de valor binário (sim ou não) usado para estudar a existência de controlos pode ser útil para encontrar a existência de controlos, mas não mede o desempenho de tais controlos. A utilização de técnicas estatísticas como a média dos valores pode não ser adequada em alguns casos, uma vez que pode simplesmente ignorar os controlos de baixo desempenho, uma vez que os resultados médios correspondem ao resultado desejável. Os pontos acima referidos concluem, assim, o problema que existe na medição da eficácia e da eficiência das medidas de segurança das TI (Aven, 2013; Fazlida, 2015; Perçin, 2008).

A primeira pedra na fundação de uma cultura de segurança e de gestão do risco em TI eficaz é definir uma visão partilhada para a segurança e objetivos claros, alinhados com a estratégia global da organização. Integrar as atividades de segurança da informação com objetivos organizacionais e obter o compromisso de uma gestão de topo para a segurança da informação é uma condição necessária, embora não suficiente, para garantir os recursos necessários e a eficácia das atividades de segurança da informação (Barafort et al., 2018; Varga et al., 2021).

São propostas várias abordagens para o alcance de uma cultura de segurança e de gestão do risco em TI eficaz. A norma de referência para a segurança da informação ISO/IEC 27001:2013, utiliza a abordagem PDCA estabelecida para impulsionar a melhoria contínua. Nesta abordagem, a auditoria é a ferramenta de gestão que proporciona às partes interessadas uma confiança razoável na consecução dos objetivos organizacionais. A abordagem moderna da auditoria vai além da identificação das não conformidades com os requisitos e, os resultados das auditorias, são, a par da monitorização dos processos e das métricas de desempenho, um dos principais impulsionadores da melhoria contínua de um sistema de gestão da segurança da informação (Meriah e Arfa Rabai, 2019).

Esta abordagem tem, no entanto, um grande inconveniente, a auditoria centra-se principalmente no cumprimento das políticas e das melhores práticas, perdendo, assim, oportunidades de melhoria proactiva destinadas a alcançar um estado de excelência em matéria de segurança. Além disso, a eficácia da auditoria como motor de melhoria está fortemente dependente das competências pessoais do auditor e da qualidade do processo. Um estudo argumenta que os benefícios da auditoria dependem de vários fatores que vão desde o conhecimento técnico dos auditores e forma de auditoria, favorecendo o aconselhamento sobre a conformidade, até ao apoio de gestão de topo e a atributos organizacionais como o ambiente regulamentar ou a eficácia da comunicação interna (Barafort et al., 2017; Everett, 2011; Meriah e Arfa Rabai, 2019).

É, ainda, argumentado que, tendo em conta a multiplicidade de normas e orientações para a gestão da segurança da informação, as organizações enfrentam uma tarefa difícil na seleção da mistura certa de documentos de referência para impulsionar o desenvolvimento e o funcionamento de um sistema de gestão da segurança da informação que equilibre a conformidade regulamentar e a redução da exposição ao risco com a otimização dos custos e impulsionando o desempenho organizacional. Embora a escolha das orientações seja influenciada pelo contexto organizacional e por fatores subjetivos, a variedade de referências dificulta o *benchmarking* da segurança em diversos ambientes ou organizações (Everett, 2011; Hohan, 2015).

Uma abordagem diferente proposta por diversos autores assenta na aplicação de modelos de avaliação da maturidade. Os modelos de avaliação da maturidade são um conjunto estruturado de critérios que descrevem a capacidade dos comportamentos e processos de uma organização para produzir os resultados desejados de forma fiável e sustentável. A maturidade pode ser usada como referência para comparação e como uma ferramenta para compreender as melhores práticas e alcançar o cumprimento de um conjunto de requisitos. São identificados quatro modelos complementares para avaliar a maturidade da segurança sendo estes o "Modelo de Maturidade de Capacidade de Engenharia de Segurança de Sistemas da Organização Internacional de Normas", o "Guia do NIST para a Avaliação dos Controlos de Segurança", "Objetivos de Controlo das Tecnologias da Informação" e o "Modelo de Maturidade de Gestão de Segurança de Informação Aberta"(Chou, 2007; M, 2001).

O Modelo de Maturidade de Capacidade de Engenharia de Segurança centra-se nas práticas de segurança e avalia a maturidade através da sua fiabilidade e sustentabilidade, desde práticas informais a práticas definidas, controladas e continuamente melhoradas.

O Guia do NIST para a Avaliação dos Controlos de Segurança (NIST, 2013) centra-se nas políticas, procedimentos e controlos técnicos, bem como nas suas implementações. A avaliação da maturidade começa na definição de regras e responsabilidades gerais, no nível máximo de maturidade, as políticas, os procedimentos e os controlos são implementados, testados e melhorados regularmente. Deste modo a segurança das TI está incorporada na cultura corporativa e nas práticas do dia-a-dia.

Os Objetivos de Controlo das Tecnologias da Informação do ISACA (COBIT) (IT Governance Institute, 2007) focam-se na gestão dos riscos. A maturidade da segurança da informação é avaliada pela capacidade do quadro de gestão do risco associado. No nível básico, os riscos são considerados e tratados de forma *ad hoc.* Na maturidade de nível superior, a gestão dos riscos é um processo estruturado, organizacional e bem gerido, sendo que, a segurança das TI está integrada com os objetivos do negócio de segurança corporativa.

O Modelo de Maturidade de Gestão de Segurança de Informação Aberta (Open Group, 2011) define um quadro abrangente de processos de segurança, com processos abrangendo diferentes níveis de governação da organização como processos genéricos, gestão estratégica, gestão tática e gestão operacional. Este também define métricas de procedimentos usadas para avaliar o desempenho do processo em si. A sua definição de níveis de maturidade baseia-se numa seleção específica construída em relação aos processos em vigor e eficazes na organização.

Um quadro da comparação entre os modelos de maturidade enunciados encontra-se representado na Figura 2.2.

Security Maturity Model	Maturity levels	Focus theme	Top maturity level
Systems Security Engineering Capability Maturity Model (ISO, 2008)	1-5	Security practices	Continual improvement of security practices
Control Objectives for Information Technology – COBIT (IT Governance Institute, 2007)	0-5	Risk management	Optimized: Risk assessment as a structured, organisation-wide and well-managed process. Integration of IT security with corporate security business objectives
information security technology assessment framework - NIST 800-53 (NIST, 2013)	1-5	Policies, procedures, controls	Integration: Continuous review and improvement of policies, procedures and controls. Integration of IT security into corporate culture and practices
Open Information Security Management Maturity Model (Open Group, 2011)	Initial, Managed, Defined, Controlled, Optimized	Processes	Specific per category of process. Definition of processes on highest level (optimized) include specific practices for implementation, testing, monitoring, planning, realisation of benefits, assessment and optimisation (continuous improvement) of the process.

Sources: (NIST, 2013; IT Governance Institute, 2007; ISO, 2008; Open Group, 2011)

Figura 2.2 - Comparação dos modelos de maturidade de segurança em TI (Barafort et al., 2017)

Os modelos de avaliação de maturidade definem claramente um caminho para um sistema de segurança da informação maduro, no entanto, não se encontram alinhados com a estratégia e objetivos organizacionais globais. Devido a tal, são úteis até que um determinado nível de cumprimento de um conjunto de regras ou boas práticas seja alcançado, como um padrão legal. Após o cumprimento, e a segurança da informação ser "madura", o poço de melhorias seca e são necessárias novas ferramentas para procurar uma melhoria contínua e um alinhamento proativo da postura de segurança para novos desafios e requisitos de segurança. Ademais, a validade das conclusões retiradas das avaliações de maturidade e a eficácia das ações incorridas são diretamente influenciadas pela adequação da referência, do conjunto de regras, requisitos e boas práticas, para a organização e para o seu contexto (Hohan, 2015).

3. METODOLOGIAS PARA GESTÃO DO RISCO EM TI

Não existe um método específico para a gestão do risco em TI, porém há processos comuns que devem ser executados de forma a proporcionar uma gestão eficiente. O estabelecimento do contexto da gestão dos riscos, a análise dos riscos e a monitorização e revisão dos mesmos são processos comuns a toda a metodologia de gestão de risco descrita na NIST 800-30 e na ISO 27005:2018 (Fikri et al., 2019). Neste caso em concreto vai ser dado ênfase ao ciclo PDCA, utilizado como apoio à aplicação da FMEA para suportar a metodologia criada de implementação da abordagem GRC no Grupo EDP, devido à flexibilidade aplicacional e organizativa do primeiro e devido à capacidade de diminuição da frequência de falhas, ou até mesmo eliminação, do segundo (Cicek e Celik, 2013; Zohuri e McDaniel, 2021). Nos pontos seguintes são, então, explicadas as metodologias selecionadas para a implementação da abordagem GRC assim como o conceito da abordagem em si, como é feita uma correta implementação empresarial e técnica e quais os fatores críticos ao sucesso da mesma.

3.1. Ciclo PDCA

O ciclo PDCA, proposto por W.E. Deming, um estatístico americano, é um método lógico cuja intenção assenta na melhoria da eficácia na execução de uma série de atividades. Foi usado pela primeira vez no campo da gestão da qualidade (Song e Fischer, 2020). Posteriormente, foi aplicado em muitas áreas de gestão onde foram obtidos resultados favoráveis. Refere-se, assim, a uma abordagem ao processo de gestão ou ao ciclo de aprendizagem da descoberta. É uma das pedras angulares do mundo da qualidade, da norma ISO 9001 (Zohuri e McDaniel, 2021).

O ciclo PDCA, como método de gestão iterativo estabelecido para proporcionar melhoria em processos, centra-se na aprendizagem contínua e criação de conhecimento e é implementado através de uma lógica de ciclo (Jones et al., 2010). O ciclo PDCA assenta na combinação das primeiras letras de "Plan", "Do", "Check" e "Act", também conhecido como ciclo de qualidade, sendo este um modelo geral dentro dos modelos de gestão. O ciclo PDCA pode ajudar a diferenciar uma empresa comparativamente aos seus concorrentes, particularmente

no mundo empresarial atual, onde, as empresas procuram constantemente novas formas de agilizar processos, reduzir custos, aumentar lucros e melhorar a satisfação dos clientes (Jiang et al., 2021; Song e Fischer, 2020).

Aplica-se o ciclo PDCA quando é iniciado um novo projeto de melhoria, desenvolvido um novo *design* ou melhorado um processo, produto ou serviço. Inclui ainda outras aplicações como a definição de um processo de trabalho repetitivo, o planeamento da recolha e análise de dados para verificar e priorizar problemas ou causas-raiz, a implementação de alterações e trabalhos relativos a melhoria contínua. As empresas que procuram melhorar os seus processos internos e externos muitas vezes implementam a metodologia PDCA para minimizar erros e maximizar os resultados. Uma vez estabelecido, as empresas podem repetir o ciclo e torná-lo um procedimento operacional padrão. A fase final da metodologia, "Act", toma ações corretivas e torna a metodologia ideal para esforços de melhoria contínua.

O ciclo PDCA compreende 4 fases: Plan, Do, Check e Act (Sangpikul, 2017):

Na fase "Plan", uma equipa identifica um desafio que pretende ultrapassar ou uma oportunidade que espera aproveitar. Consequentemente, a fase de planeamento envolve avaliar um processo atual, ou um novo processo, e calcular, de um ponto de vista exterior, como pode ser melhorado. Saber o tipo de efeito desejado ajuda a desenvolver um plano para corrigir ou melhorar o processo. Muitas vezes é mais fácil planear mudanças menores durante esta fase do ciclo para que possam ser facilmente monitorizados, e para que os efeitos sejam mais previsíveis (Zohuri e McDaniel, 2021).

A fase "Do" é a oportunidade da equipa testar a sua ideia de mudança. Esta fase normalmente inclui uma pequena experiência ou teste. Este é o passo em que o plano está em andamento. Esta fase pode ser dividida em três subsegmentos, incluindo a formação de todo o pessoal envolvido no projeto, o processo real de realização do trabalho e o registo de *insights*, ou dados, para futura avaliação. É de notar que, na presente dissertação, a aplicação prática deste conceito do ciclo PDCA é reformulada e personalizada ao caso prático do Grupo EDP, como explicado na Secção " 4.2. Plano de Implementação GRC", do Capítulo 4.

Na fase "Check" do ciclo PDCA, o negócio reúne e avalia os resultados experimentais. Na eventualidade destes se revelarem bem-sucedidos, a empresa implementa a mudança a uma escala mais ampla. Caso contrário, a empresa pode voltar à fase "Plan" e traçar um plano diferente (Jiang et al., 2021).

Geralmente, deve haver dois tipos de controlos integralmente no projeto. Em primeiro lugar, controlos a par da implementação, ou seja, controlos que garantam que os objetivos do projeto estão a ser atingidos. Em segundo lugar, controlos que permitam uma revisão mais abrangente do projeto. O segundo tipo deve ser realizado após a conclusão de forma a abordar os êxitos e falhas, assim, é possível efetuar ajustamentos futuros (Sangpikul, 2017).

Na fase "Act", o passo final do ciclo PDCA, um negócio toma medidas corretivas de acordo com os conhecimentos que obteve após análise da experiência obtida nas fases anteriores. A empresa pode, portanto, implementar a mudança a níveis superiores quando esta é satisfatória. Em casos onde a expectativa fique aquém, a empresa poderá ter de voltar ao início do ciclo, à fase de "Plan", no sentido de testar outras hipóteses de processo. O ciclo PDCA é

repetido e pode ser redefinido com o fim de obter melhores resultados sob novas orientações (Jones et al., 2010; Zohuri e McDaniel, 2021).

3.2. FMEA

A metodologia FMEA foi desenvolvida e aplicada pela primeira vez em 1949 pelo United States Army (Scipioni et al., 2002). Na década de 1970, graças às suas características de eficiência na análise de risco de insucesso, o campo de aplicação da mesma estendeu-se. Primeiramente alargou-se à indústria aeroespacial e automóvel, depois à indústria aeronáutica e a áreas cada vez mais diversas, como a indústria química, engenharia ambiental e indústria marinha (Cicek e Celik, 2013; Yazdi et al., 2020).

3.2.1. Conceitos Fundamentais da Metodologia FMEA

Falha - Existe uma falha quando um produto, sub-produto ou componente não satisfaz, não cumpre uma função ou não funciona de acordo com as especificações.

Modo de Falha - Modo como se produz uma falha de um produto ou componente.

- Na metodologia FMEA é necessário identificar, para cada uma das funções do produto, todos os modos possíveis de falha.

Efeito - Consequência, no produto ou no componente, da ocorrência do modo de falha;

- Na metodologia FMEA é necessário analisar, para cada modo de falha, os efeitos sobre o componente e produto.

Causa - Deficiência do sistema que provoca um determinado modo de falha;

- Na metodologia FMEA é necessário identificar, para cada modo de falha potencial, as suas causas (H. Li et al., 2021).

A FMEA como metodologia examina as consequências ou efeitos de falha num sistema, nas pessoas ou no ambiente (Hassan et al., 2022). Pode ocorrer mais do que um efeito para cada modo de falha, mas, normalmente, a equipa de FMEA concentra-se no efeito com o impacto mais sério para a análise (Liu et al., 2011). É, assim, uma abordagem *bottom-up* para a análise de risco e uma metodologia competente para um modelo de risco completo. A FMEA apoia decisões qualitativas de identificação de riscos no desenho e durante as operações no âmbito da inspeção baseada em risco, seguindo orientações como a API 581 (2016) (Pillay e Wang, 2003).

Esta metodologia pode ser aplicada em todas as fases do ciclo de vida de um projeto, incluindo conceção, instalação, operações e desmantelamento. A FMEA, quando utilizada durante a fase de conceção, tem o potencial de pré-identificar potenciais falhas evitando, assim, remodelações de projeto dispendiosas ou permitindo que as fraquezas sejam identificadas e retificadas antes de colocar o projeto em prática (Ben-Daya e Raouf, 1996).

A FMEA analisa fatores de risco do sistema e compara o grau de risco relativo a cada um através da exploração dos modos de avaria e consequentes efeitos com o objetivo de identificar eventos-chave de risco e orientar a prevenção e controlo de riscos (Jaderi et al., 2019). Para medir o grau de risco dos modos de falha, a FMEA tradicional define uma métrica de

avaliação nomeada como o Número de Prioridade de Risco (RPN). Esta deriva do produto de três classificações, Ocorrência (O), Gravidade (G) e Deteção (D) (Jianxing et al., 2021). Do cálculo do RPN resulta uma hierarquia da criticidade das falhas identificadas e pode ser calculada por números qualitativos aparentando os três parâmetros, muitas vezes baseados na opinião de peritos, dados de históricos de perda e na experiência anterior da equipa reunida. Cada um dos três parâmetros tem um ranking numérico, que tem associado uma explicação qualitativa para cada um dos números do ranking. O *ranking* e a respetiva representatividade é geralmente acordada com a equipa reunida antes do início da análise e avaliação (Li et al., 2021). Não há um padrão para a escolha do *ranking* de escala, mas, a pontuação mais comumente escolhida para efeitos de medição assenta numa escala discreta de 10 pontos, no entanto, tal escolha pode ser reconsiderada tendo em conta as características do projeto e processos em questão (Scipioni et al., 2002).

Um valor elevado do RPN implica um alto nível de risco sendo que o foco da equipa deve ser nos modos de falha correspondentes ao grau de risco em questão (Filz et al., 2021). Como técnica importante de avaliação dos riscos, a FMEA fornece de facto informações valiosas aos engenheiros de segurança e riscos para a melhoria da segurança e fiabilidade do sistema (Gargama e Chaturvedi, 2011).

O *design* e implementação da FMEA requer um conhecimento atento e vasto do sistema. Antes de relatar o resultado da aplicação prática da FMEA, é importante salientar que a primeira fase do trabalho consiste na recolha extensiva de dados e informações (Li et al., 2021).

Acrescenta-se ainda que em muitos processos práticos de avaliação de risco, é difícil para os membros da equipa da FMEA avaliar modos de falha com valores específicos devido à incerteza e à confusão do pensamento humano. Em vez disso, é mais adequado avaliar o risco segundo termos linguísticos ou quanlitativos (Jianxing et al., 2021). Centrando a atenção na incerteza e na confusão nos julgamentos linguísticos, muitas técnicas têm sido estudadas para transformar as opiniões dos especialistas em expressões matemáticas computáveis, tais como conjunto fuzzy, conjunto de confusos intuicional, Z-numbers, Teoria de Dempster-Shafer, etc (Boral, 2021; Kalathil, 2020; Kumar, 2020; Pouyakian, 2021). Entre eles, o conjunto confuso é a teoria da incerteza mais popular utilizada para representar os julgamentos linguísticos e lidar com a confusão (Liu et al., 2019). No entanto, o conjunto difuso é, muitas vezes, referido como semdo incapaz de refletir a aleatoriedade de conceitos. Considera-se, assim, ideal a utilização de conceitos qualitativos e valores quantitativos intercambiáveis para a correta e realista avaliação do grau de risco (Q. Song, 2021; Wang et al., 2021).

3.2.2. Principais Tipos de FMEAs

São, em seguida, apresentadas os principais tipos de FMEA (Filz et al., 2021; Gargama e Chaturvedi, 2011):

FMEAs de *design* (DFMEA) - São utilizadas para analisar um produto durante a fase de *design*. O principal objetivo é o de verificação e mitigação dos efeitos críticos das falhas antes das fases de fabricação e implementação.

FMEAs de processo (PFMEA) - FMEAs de processo são usadas para análise e cumprimento de objetivos de controlo de processo. Essencialmente, PFMEAs são executadas num processo e não num produto, como acontece com as DFMEAs.

FMEAs de serviço - Assentam no estudo sobre um serviço que se pretende fornecer ou criar para atender às necessidades de clientes.

FMEAs de *software* - As FMEAs de *software* são realizadas de forma a analisar os possíveis modos de falha de um *software* e os efeitos resultantes das falhas identificadas no sistema. À medida que a amplitude e a profundidade dos *softwares* aumentam nos sistemas atuais, as FMEAs de *software* podem ser de vital importância para abordar todos os caminhos de falhas potenciais.

FMEAs de fabricação/manufatura - FMEAs de manufatura ou fabricação são semelhantes às FMEAs de processo visto que exploram as falhas potenciais associadas a um processo de manufatura.

FMEAs de sistema/funcionais - FMEAs funcionais, às vezes chamadas de FMEAs de sistema, averiguam as funções de um sistema. Anteriormente à finalização de um projeto, os requisitos funcionais do mesmo podem ser aplicados como base à concretização de uma FMEA funcional.

3.2.3. Procedimento da Metodologia FMEA

Os métodos de aplicação da FMEA podem diferir ligeiramente, no entanto, há fases típicas comuns aos vários métodos.

Primeiramente deve ser feita a constituição de uma equipa multifuncional de pessoas com diversos conhecimentos sobre o processo, produto ou serviço e sobre as necessidades do cliente. Normalmente o número de elementos é de 5, 7 ou 9 pessoas, das quais é nomeado um responsável pela coordenação da equipa, esta deve estar motivada, disposta a participar e possuir espírito de grupo. As funções frequentemente incluídas são funções relativas a projeto, fabricação, qualidade, teste, fiabilidade, manutenção, compras e fornecedores, vendas, *marketing* e atendimento ao cliente. É fundamental que a equipa sinta o apoio da gestão de topo e, sempre que necessário, o cliente ou o fornecedor deve participar nas atividades necessárias (Yazdi et al., 2020).

Em seguida deve ser identificado o propósito da FMEA, ou seja, o tipo de FMEA que se tenciona aplicar, quais os seus limites e o nível de detalhe que se pretende atingir. Para tal, deve ser feita a recolha e análise de informação. É essencial obter o conhecimento rigoroso dos requisitos do cliente e das conclusões dos relatórios de reclamações, falhas, inspeções e auditorias, etc. Se aplicável, é recomendado o estabelecimento de prioridades de implementação da FMEA (Cicek e Celik, 2013; Gargama e Chaturvedi, 2011).

Para a análise funcional da metodologia FMEA, passo análogo a uma análise de valor, devem ser identificadas as funções que o produto ou processo deve desempenhar para satisfazer os requisitos do cliente. Nesta fase é normal a subdivisão em subsistemas como peças, montagens ou etapas de processo separados. Após a decomposição, se necessária, são novamente listadas as funções.

Após a análise funcional segue-se a identificação de modos de falha. Neste momento, averigua-se como pode o produto ou processo deixar de cumprir as suas funções. Para cada

função, são reconhecidas todas as maneiras pelas quais a falha pode acontecer. São, então, reconhecidos os potenciais modos de falha. Os modos de falha devem ser descritos em termos físicos e técnicos pelo que, são incluidos modos de falhas que podem ocorrer sob certas condições ambientais como calor, frio e humidade (Filz et al., 2021).

Para cada modo de falha, são posteriormente identificadas todas as consequências no sistema, sistemas relacionados, processo, processos relacionados, produto, serviço, cliente ou regulamentos. As consequências apresentam-se como efeitos potenciais de falha (Scipioni et al., 2002). Para cada modo de falha, são ainda determinas todas as causas raiz potenciais, ou seja, as causas que o podem provocar. Por cada causa, são, por fim, indicados os meios de controlo de processo existentes atualmente na organização. Estes podem ser testes, procedimentos ou mecanismos para evitar que as falhas se comcretizem ou alcancem o cliente. Os controlos podem impedir que a causa aconteça, reduzir a probabilidade de que aconteça ou detectar a falha após acontecer, idealmente sempre antes que o cliente seja afetado.

Em seguida é feita a avaliação dos parâmetros necessários ao cálculo do RPN, ou seja, da gravidade de cada efeito, da probabilidade de ocorrência de cada falha e da deteção de cada controlo. O resultado fornece orientações para classificar as falhas potenciais pela ordem em que estas devem ser tratadas, levando, assim, a uma prioritização das mesmas (Wang et al., 2021).

Face aos resultados obtidos, deve ser elaborado um plano de ações corretivas que privilegie a prevenção. É, então, nesta fase final que são constatadas as ações recomendadas que podem abranger modificações de design ou processo de forma a reduzir a gravidade ou a ocorrência. Podem ainda ser adicionados novos controlos complementares com o objetivo de melhorar a deteção. Às medidas de melhoria deve ser designado um responsável e definir um prazo de implementação para cada ação corretiva. Após implementação das acções corretivas, são novamente calculados os RPNs. Caso não tenha existido uma ação corretiva para um determinado potencial modo de falha, o respetivo RPN mantém-se em branco (Hassan et al., 2022; Jianxing et al., 2021; Pillay e Wang, 2003).

3.3. Abordagem GRC

3.3.1. Definição da Abordagem GRC

O GRC é um conjunto multidisciplinar de aplicações que são projetadas para mudar a visibilidade do risco e o ponto de vista da conformidade, atuando assim na unidade de gestão do risco de uma empresa. Resulta, portanto, da integração de quatro áreas do conhecimento, representadas e descritas na Figura 3.1, sendo estas a gestão de políticas e conformidade, gestão do risco, gestão das auditorias e gestão do risco do fornecedor. É relevante evidenciar ainda que, GRC deve ser compreendido dentro de um contexto global, sendo importante evitar a sua análise separada de conceitos. Este contexto global de gestão do risco visa garantir a conformidade regulamentar e responder à imposição de normas internacionais, consolidando-as dentro de um único modelo que unifique os interesses internos e externos de uma organização.

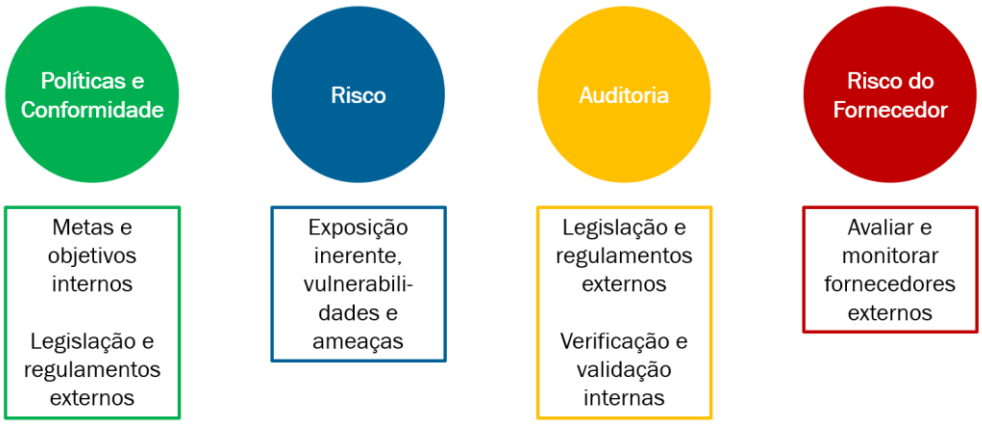


Figura 3.1 - Áreas de Conhecimento da Abordagem GRC

No contexto de gestão empresarial, o GRC consiste numa metodologia que envolve a integração dos processos de uma empresa de maneira clara, unificada e segura (Ramalingam et al., 2018). O objetivo é garantir a conformidade das operações e políticas corporativas com o que está previsto na lei e outros regulamentos. Como *output* do GRC, obtém-se uma visão geral da posição real da empresa relativamente às ações que deveriam ocorrer *versus* as que realmente são aplicadas, assim como dos riscos que são elevados ou mitigados por essas mesmas ações. Tal visão é possível através da realização de auditorias que confirmam, de forma objetiva, os processos implementados (Aven e Krohn, 2014).

A metodologia GRC baseia-se na articulação de três práticas, *governance, compliance* e risco, e na sua implementação nas atividades corporativas (Fazlida, 2015).

3.3.1.1. Governance

A primeira prática refere-se à forma como é gerida a tomada de decisão pelos gestores de topo e líderes das empresas. Nesta prática está envolvida uma estratégia de criação e implementação de políticas, normas e procedimentos internos cuja finalidade é a orientação das equipas de diversos departamentos para a realização de um trabalho claro, transparente e seguro.

3.3.1.2. Compliance

A área de conformidade diz respeito à necessidade de as atividades desenvolvidas pela empresa obedecerem às normas e legislações instituídas. Para esse fim, deve ser efetuada uma revisão contínua sobre as operações.

3.3.1.3. Risk

A última prática assenta na análise completa sobre as operações da organização com o objetivo de identificar as possíveis falhas e vulnerabilidades existentes nos procedimentos e atividades. Estas, assim como incumprimentos de regulamentos legais, podem causar prejuí-

zos à empresa. Nesta análise são também considerados os diversos níveis de impacto e probabilidade dos riscos, decorrentes das falhas, vulnerabilidades ou incumprimentos, de forma a ser possível uma classificação real e priorização dos mesmos (Kremljak e Kafol, 2014).

Podem ocorrer diferentes tipos de risco. Neste sentido, a gestão dos riscos tem capacidade de ajudar a identificar o que é mais importante salvaguardar, avaliar os impactos que os riscos podem provocar e, então, colocar medidas em prática a fim de evitar ou, pelo menos, reduzir as consequências negativas que estes podem induzir nos negócios.

3.3.2. Benefícios da Abordagem GRC nas TI

Os benefícios da correta implementação GRC encontram-se nas melhorias nos controlos de acesso e processos de administração de utilizador, melhorias na eficácia e eficiência das atividades de controlo existentes, automação das atividades de controlo utilizando controlos contínuos de monitorização. Inclui ainda a capacidade de demonstrar a eficácia operacional dos controlos através da implementação de um repositório de controlos comum para ambas as documentações e operação dos controlos e redução do esforço necessário para testar os controlos, tanto da perspetiva de auditoria interna como externa (Hunt, 2014).

Permite, portanto, obter um alinhamento estratégico visto que garante sintonia entre a área de segurança de TI e as estratégias do negócio. Para além disso, acrescenta valor a esta área, uma vez que a sintonia mencionada é vista, também, de forma estratégica. O GRC garante, também, a transparência da gestão dos ativos sendo possível criar inventários dos recursos tecnológicos usados pela organização e controlar, de forma eficaz, o seu funcionamento.

Acrescenta-se, por fim e como benefício, a possibilidade de monitorização do desempenho dos ativos adotados, através do acompanhamento contínuo de índices de performance. A agregação de todas estas vantagens leva a que a área de segurança de TI aplique ferramentas estratégicas com o propósito de atingir as metas delineadas para a empresa.

3.3.3. Aplicação da Abordagem GRC em TI

O primeiro passo, que promove o sucesso da aplicação da abordagem GRC, assenta na sua comunicação e aceitação por parte de toda a empresa visto que está baseada numa nova visão de gestão dos ativos de TI. Neste passo, é importante dar relevância aos benefícios que esta prática pode significar para a organização e a potencialidade no auxílio em termos de crescimento e segurança do negócio e das respetivas atividades e operações.

Numa visão geral é primeiramente necessário analisar a série de métodos e regulamentações que permitem o bom funcionamento das rotinas empresariais. Em seguida é feita a revisão de todos os processos aplicáveis às TI, a sua adequação e monitorização constante.

A implementação de GRC inclui quatro etapas básicas, que se encontram listadas e explicadas abaixo (Boral, 2021; Mesquida et al., 2014):

Definição de objetivos - Um dos motivos mais comuns de insucesso na implementação desta abordagem assenta na falta de definição dos objetivos que esta pretende atingir. A identificação dos mesmos pode ser construída em equipa e com os *stakeholders* interessados, sendo deste modo possível percecionar as expectativas e prioridades individuais.

Análise da situação atual - Seguidamente à definição das metas desejáveis é necessário verificar a situação atual das áreas de *compliance*, *governance* e de gestão dos riscos. Com a análise referida é possível obter uma compreensão real e atual do estado dos processos de cada uma das áreas mencionadas e prever a melhor forma de enquadrar o GRC na organização com o fim de cumprir os objetivos delineados.

Acrescenta-se ainda, a vantagem adquirida pela revisão processual, a qual assenta na recolha de inconsistências, falhas, atividades duplicadas, etc. Situações estas possivelmente não identificadas quando da decisão de implementação do GRC.

Definição de ponto de partida - É recomendado, na maioria dos casos, que a implementação da abordagem GRC envolva a totalidade dos processos de uma organização. Porém, esta pode e deve ser feita de forma faseada e por setores ou departamentos. Deste modo, é possível fazer a testagem e ajuste de cada parte previamente à seguinte, sendo que, esta implementação gradual proporciona controlo e um consciente aproveitamento de todos os recursos a ser adaptados.

Monitorização - Após finalizada a implementação GRC, segue-se a monitorização contínua. Nesta fase é feito o acompanhamento dos processos intrínsecos à empresa com o intuito de obter informações imediatas sobre as forças e fraquezas momentâneas. Esta fase permite ainda verificar as necessidades de adaptação ainda não tratadas e agir de forma preventiva em relação a estas.

A etapa de monitorização é ideal para a demonstração de resultados, benefícios alcançados e para promover o interesse dos colaboradores em desempenhar um papel mais ativo na utilização deste serviço.

3.3.4. Possíveis Impedimentos de Sucesso

Um dos principais fatores de insucesso no processo de implementação da abordagem GRC encontra-se na seleção da tecnologia mais adequada às circunstâncias da empresa e mais provável de oferecer os benefícios esperados. Caso o foco seja melhorar os controlos internos, é necessário, por exemplo, um *software* de análise de controlos acompanhado por uma ferramenta de gestão de acessos privilegiados. Pode ser feita a aquisição, por parte da organização, de um *software* especializado com inúmeras funções. No entanto, não deve ser assumida uma escolha aleatória e sem ponderação prévia sobre as funções disponibilizadas no *software* em comparação com as necessárias (Hunt, 2014).

Alguns dos fatores a considerar, quando da seleção das ferramentas de GRC corretas, incluem o conhecimento dos principais futuros utilizadores deste serviço, o cenário TI existente na organização, os requisitos de integração dos componentes das infraestruturas como soluções de gestão de identidades e o nível e âmbito dos controlos automatizados necessários, assim como a necessidade de implementar controlos semiautomáticos. Acrescenta-se ainda a questão da incorporação do *software* nos cenários de TI existentes na empresa, ou na implementação de um *software* autónomo para realizar análises de dados extraídos. É, também, essencial considerar o volume de dados e os requisitos para a análise dos mesmos.

Com o propósito de ter retorno do investimento e desbloquear os ganhos na eficiência, é preciso considerar a automação de certas áreas, como a monitorização de transações, continuidade dos controlos e *user provisioning*. Estas tecnologias permitem que a organização use automação na administração do utilizador e no controlo dos processos de monitorização. A adição de processos de automação no âmbito do projeto GRC acrescenta complexidade e risco. Porém, acrescenta também melhorias significativas no negócio, em termos de retorno do investimento.

Na definição do âmbito do projeto, é também importante considerar os recursos técnicos disponíveis em comparação com o que é pragmático implantar no negócio. A inclusão inicial de soluções mais complexas pode atingir os objetivos finais do projeto, podendo, igualmente, a sua implementação ser considerada como um desafio. O sistema de negócio existente pode não estar, nem ser suficientemente preparado, para lidar com todos os recursos de uma solução de gestão do risco integrada e automatizada e, portanto, apesar da intenção *endpoint* ser a correta, pode resultar numa redução dos benefícios reais, pois as atividades não conseguem operar efetivamente. É devido a tal, que a definição de objetivos é o ponto de partida ideal em termos dos processos de implementação GRC. Desta forma, as etapas requeridas para atingir as metas planeadas, podem ser determinadas e desenhadas (Hunt, 2014).

3.3.5. Fatores Críticos de Sucesso

Em primeiro lugar, é essencial criar um *roadmap* para a abordagem GRC a implementar. Este é útil para reforçar o que a organização pretende alcançar com a iniciativa, e serve, para delinear o caminho a percorrer para atingir os objetivos estipulados, cuja importância foi anteriormente determinada na definição dos objetivos, e obter as ferramentas necessárias ao apoio desta progressão. A decisão em relação a tais ferramentas de apoio pode assentar no uso de tecnologias já existentes de forma a melhorar os processos que as operam ou na atualização para um novo GRC contemporâneo, de acordo com as vantagens possíveis para o decorrer do negócio. Esta atualização pode incluir alguns recursos recentes disponíveis como a harmonização do controlo de processos de gestão de acessos e recursos relativos a uma gestão do risco holística. Pode incluir ainda melhorias na monitorização de controlos, permitindo, assim, a automação dos mesmos, melhorias nos recursos de construção de relatórios, proporcionando acesso a painéis executivos avançados e Key Performance Indicators (KPI) de risco, melhorias no acompanhamento de transações e análises, em tempo real, de indicadores incorretos, através de alertas baseados em eventos.

Quando a automação de controlos está no âmbito de processos como a administração de utilizadores, é recomendado que a versão mais recente de qualquer produto seja considerada. Embora exista a possibilidade desta ação ser acompanhada pelos problemas comuns associados à adoção antecipada de qualquer *software*, os avanços na área da automação de controlos estão a aumentar exponencialmente, logo, as versões mais recentes da tecnologia GRC, incluirão no produto as últimas melhorias nesta área.

Uma vez determinada a tecnologia a implementar, é essencial entender que uma implementação, ou mesmo atualização para a última solução GRC, não deve ser tratada puramente

como um projeto técnico. Mesmo existindo um elemento técnico na iniciativa, o maior benefício é adquirido quando da incorporação das ferramentas GRC, pelas equipas do projeto, na organização de processos e conformidade. Ao definir *roles* e responsabilidades para o uso do *software* de aplicação do GRC e ao fornecer a formação necessária para ajudar os colaboradores a entender como usá-lo corretamente, a probabilidade de obter melhorias internas na monitorização dos controlos aumentará significativamente.

Ainda, de forma a alcançar os benefícios públicos da abordagem, é crucial confirmar a operabilidade eficaz das ferramentas em implementação. Este ponto é essencial para a harmonia entre colaboradores e processos, além da tecnologia. Deve, por isso, ser considerado como fator crítico de sucesso.

De forma a garantir este equilíbrio crítico são necessárias atividades de gestão de mudança, assim como a sua implementação técnica para entregar ao negócio os benefícios espectáveis do projeto. Para tal, devem estar incluídas uma combinação de treino e comunicação nos passos de implementação da abordagem GRC. A formação deve incluir, não só a forma de utilização da nova solução GRC, mas também a razão pela qual esta está a ser aplicada e as soluções suportadas pelos processos de GRC. A envolvência dos principais utilizadores durante o decorrer de todo o projeto, particularmente em atividades como a definição de requisitos de negócios e o teste de aceitação do usuário, pode ser um contribuidor relevante para o alcance geral da gestão de mudança e, por sua vez, objetivos do projeto (Fazlida, 2015).

Comunicações, que desempenham um papel fundamental, devem ser feitas numa lógica *top down*, sendo que, todos na organização têm um papel a desempenhar a este respeito. Uma estratégia para uma comunicação eficaz inclui o uso de linguagem corrente, que os utilizadores conseguem compreender, e a simplificação, para um nível apropriado, das ideias complexas. As mensagens, alertas e notificações correspondentes à ferramenta escolhida devem ser também adaptadas aos diferentes tipos de públicos que as recebem e deve ser claramente articulado o papel que cada grupo tem (Hunt, 2014).

3.3.6. ServiceNow

A escolha da ferramenta de apoio a esta abordagem de gestão do risco e conformidade em TI, teve em consideração os *softwares* já utilizados pelo Grupo EDP. O *software* ServiceNow foi aplicado ao longo dos anos por diversas unidades do Grupo EDP em diversas áreas, e, a seleção do mesmo teve, por isso, em conta a familiaridade dos colaborados com a ferramenta, a disponibilidade dos módulos, dentro da secção de GRC no ServiceNow, de risco e de *policy & compliance*, e a capacidades de armazenamento e transformação de dados. Uma visão geral da solução ServiceNow relativa aos módulos presentes no mesmo encontra-se apresentada na Figura 3.2. Esta dissertação recorre aos módulos de GRC para implementação da abordagem de gestão do risco em TI, consequentemente são incluidos os módulos de *risk management* e *policy&compliance management*.

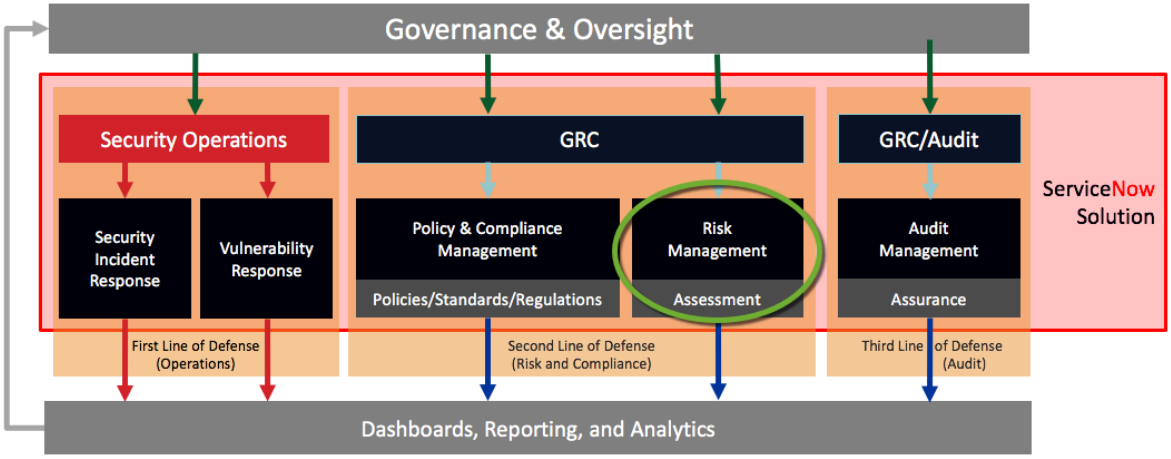


Figura 3.2 - Visão geral, esquemática, dos módulos do ServiceNow [2]

Para além dos motivos mencionados, em 2020, o ServiceNow foi um dos líderes do Quadrante Mágico de Gartner no âmbito de gestão do risco em TI, como é possível verificar na Figura 3.3. *Magic Quadrant* (MQ), ou Quadrante Mágico, combina uma série de relatórios de pesquisa de mercado publicados pela empresa de consultoria de TI Gartner. Estes relatórios têm por base métodos de análise de dados qualitativos com o objetivo de demonstrar as tendências de mercado. As análises realizadas são conduzidas para vários setores tecnológicos específicos e são atualizadas a cada um ou dois anos, sendo que, uma vez que um relatório atualizado seja publicado, o seu antecessor deixa de ter efeito (Gartner, 2021).

Figura 3.3 - Quadrante Mágico de Gartner (Gartner, 2020)

[2] https://docs.servicenow.com/bundle/rome-governance-risk-compliance/page/product/grc-policy-and-compliance/concept/policy-compliance.html

Gartner define o mercado de soluções de gestão do risco em TI como *software* e serviços que operacionalizam o ciclo de vida de gestão do risco no contexto da missão da organização. As soluções são então concretizadas para estabelecer um *hub* central que facilita a tomada de decisões relativas aos negócios e à gestão dos riscos. Os riscos rastreados geralmente são ativados como resultado de escolhas feitas em TI, operações digitais e de segurança, gestão de informações, planeamento de continuidade de negócios e gestão de conformidade de TI e segurança. Estas escolhas são orientadas por prioridades concorrentes que exigem visibilidade de risco e priorização com base nos resultados de negócios.

Cenários originados ou atribuídos a infraestruturas digitais, aplicações, sistemas, processos, projetos e equipas são objeto de análise e reporte nas soluções de *software* e serviços de gestão do risco em TI (Gartner, 2021).

Os fornecedores no quadrante dos "Líderes", caso do *software* escolhido para a implementação da abordagem GRC no Grupo EDP, ServiceNow, têm as pontuações mais altas para a "Completude de Visão" e "Capacidade de Execução". Um fornecedor no quadrante dos "Líderes" considera-se que tem participação no mercado, credibilidade e os recursos de *marketing* e vendas necessários para impulsionar a aceitação de novas tecnologias. Os fornecedores nesta posição demonstram uma compreensão clara das necessidades do mercado, são inovadores e líderes de pensamento e têm planos bem articulados que os clientes atuais e potenciais podem usar ao projetar as suas infraestruturas e estratégias. Acrescenta-se ainda outros fatores como a presença nas cinco principais regiões geográficas, um desempenho financeiro consistente e amplo suporte na plataforma informática ou *software* que vendem (Gartner, 2021).

Segundo o relatório do MQ de Gartner, em 2020, a ServiceNow esteve focado em aprimorar os próprios recursos de avaliação de risco, dando, assim, suporte a um número crescente de tipos de avaliação de risco prontos para uso e automação na área de monitorização de controlos (Gartner, 2020).

Reportou-se, ainda, que os clientes atribuem as características de funcionalidade e desempenho do produto como os principais motivos para selecionar o ServiceNow. O feedback do cliente indica que integrações avançadas, descoberta de ativos digitais e avaliações quase em tempo real, em particular, excedem as expectativas iniciais (Gartner, 2020).

3.3.6.1. Como Aplicar GRC no ServiceNow

O objetivo da abordagem GRC é garantir que a empresa tem conhecimento de todas as entidades do sistema que não só apresentam risco como precisam de ser mantidas em conformidade. Entidades podem ser servidores, departamentos, indivíduos, aplicações, entre muitos outros.

Deve ser feita uma configuração inicial, um esquema dos elementos necessários à mesma encontra-se na Figura 3.4. Este processo pode representar cerca de 90% do projeto em si, tendo em conta a existência de inúmeros documentos de processo de negócio, tanto de legislação externa como políticas e normas internas, que, após análise detalhada, resultam na criação de controlos. Estes representam as ações a ser tomadas a um nível rotineiro. Nesta fase é também criada a estruturação dos riscos que a empresa enfrenta ou pode enfrentar e a declaração dos mesmos. Ainda, é feita a organização de todas as entidades participantes no sistema da organização, as quais devem ser previamente listadas e posteriormente classificadas de forma a que a sua correlação com os riscos encontrados e controlos enunciados seja assertiva.

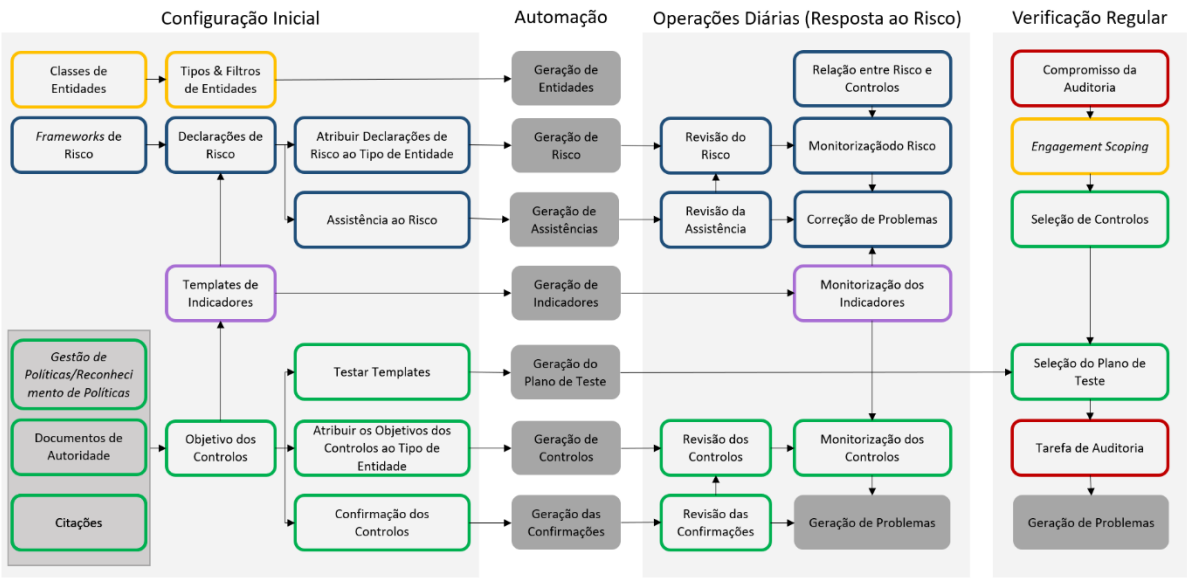


Figura 3.4 - Esquema da configuração inicial do ServiceNow

Após a integração de toda a informação reunida durante a configuração inicial, esta é inserida no sistema ou *software* autónomo que procede à automação da gestão do GRC. Como resultado, obtém-se a geração, pelo *software*, de indicadores, riscos e a assistência necessária a estes. Esta arquitetura em constante mudança é feita, automaticamente, em tempo de trabalhado dos colaboradores permitindo assim a otimização das suas tarefas diárias e resposta ao risco pois, quando de qualquer alteração, os trabalhadores são notificados. Esta operação automática, possibilita ainda uma monitorização direta, simples e diária dos resultados vigentes por parte dos gestores de risco e conformidade visto que assenta em informação sempre atualizada e disponível.

Como se pode observar na Figura 3.4, encontra-se, por fim, a parte da auditoria que representa a verificação regular da qualidade do desenho dos controlos e da qualidade da sua implementação dentro das operações diárias da empresa. Esta etapa pretende avaliar a necessidade de executar novas alterações não só no desenho de controlos como também nos processos onde os mesmos são aplicados.

3.3.6.2. Módulo do Risco do ServiceNow

O GRC funciona como um todo. Um dos módulos integrantes, o módulo do risco, inicia-se com a estrutura subjacente "Entidade". A entidade é simplesmente um registo no ServiceNow que é considerado como uma possibilidade de apresentar risco, uma aplicação, um servidor, um departamento, um processo de negócio, um indivíduo, etc. Estas são todas as entidades que hipoteticamente podem apresentar risco para a empresa, sendo que as mesmas são abordadas no *software* através da construção de "*Frameworks* de Risco", "Declarações de Risco" e os próprios "Riscos".

As *frameworks* de risco assentam na ideia de uma categorização personalizada das entidades listadas e pertencentes a uma organização. Podem ser criadas *frameworks* de riscos ambientais, riscos de controlo de acesso, riscos de processos de negócios departamentais ou riscos humanos, entre outras. Estas aplicam-se, assim, como forma de categorizar os dados dispersos.

A declaração de risco é a visão da empresa. Citando caso análogo, na análise de um possível risco de exposição da empresa a incêndio, a avaliação do mesmo não é feita para o total da organização. É abordado o risco de incêndio para todas as partes que compõe a organização, é, portanto, abordado o risco de incêndio em cada instalação e em cada *data center*. De referir ainda, como outro exemplo, o problema do controlo de acesso inadequado a sistemas ou à rede, este qual pode levar à exposição de informações pessoais não ao nível da empresa mas sim ao nível de cada aplicação. É nesta relação com as entidades que a declaração de risco se converte num ou vários riscos, dependente, neste caso, do número de aplicações consideradas para este efeito. Os riscos são gerados pelo ServiceNow automaticamente, onde, o tipo de entidade é basicamente o *hub* onde são definidas todas as relações entre os riscos. O sistema identifica, automaticamente, as entidades que necessitam de monitorização, analisa as declarações de risco da empresa relacionadas com as entidades monitorizadas e gera os próprios riscos respetivos.

Como forma de avaliação do risco gerado automaticamente, é obtida a perspetiva dos colaboradores, ou seja, dos indivíduos responsáveis pelas entidades em questão. Tal é obtido através do simples envio de assistências ao risco. Estas incluem um pedido de avaliação do risco que é depois devolvido pelos utilizadores. Após devolvida a assistência ao risco, segue-se a etapa de aceitação da perspetiva de avaliação do risco recebida, todo este processo é, então, um processo manual. O risco é assim atualizado para um estado de revisão onde ocorre a decisão de resposta ao mesmo, em conjunto com os parceiros de negócio, e quais as diversas tarefas envolvidas na resposta. Este trabalho manual permite que a equipa de gestão seja envolvida na configuração inicial, definindo as estruturas, as declarações de risco e construindo a avaliação de risco de forma a que sejam colocadas as perguntas adequadas quando o envio de assistências ao risco.

De forma a obter a verdadeira mitigação do risco, o processo decorrente no módulo de risco é construído lado a lado e relacionado com o processo decorrente no módulo de *policy & compliance*. Esta estratégia permite correlacionar os controlos aos riscos. Assim, a ideia de manter a conformidade coesa com os controlos impacta diretamente o risco residual que resta.

3.3.6.3. Módulo de *Policy & Compliance* do ServiceNow

Este módulo surge como conceito de conformidade com os requisitos legais. O módulo de *policy* & *compliance* do ServiceNow fornece um processo centralizado para a gestão de políticas, normas e procedimentos de controlo interno. Estes são mapeados de forma cruzada com regulamentos externos e boas práticas publicadas. Este é, assim, o lado interno da conformidade, onde as políticas internas são a forma como as coisas são feitas na empresa de acordo com o setor em que se encontra e o negócio em si. A conformidade inclui não apenas as questões internas mas também as externas. Estas últimas incluem regulamentações externas cuja origem provém de vários órgãos reguladores internacionais. O módulo fornece, ainda, fluxos de trabalho estruturados para identificar entidades no ServiceNow que precisam de ser mantidas em conformidade, avaliá-las regularmente e monitorá-las continuamente num horário regular automatizado de atividades de controlo.

A configuração inicial do módulo processa-se com a documentação de autoridade, sendo, neste ponto, analisadas as fontes regulatórias internas e externas, ou seja, os "Documentos de Autoridade". Num documento de autoridade, cada seção que fornece conteúdo testável nesse documento é considerada uma "Citação", são estas que são mapeadas para as políticas internas. A forma como são geridas as políticas encontra-se na função "Reconhecimento de Políticas" do ServiceNow.

Relativamente aos "Controlos", estes são criados para testar a conformidade com requisitos por parte da organização, dado que, o "Objetivo de Controlo" é um parâmetro no nível corporativo que reflete o estado da organização no momento em termos de conformidade. Estes parâmetros de conformidade, os objetivos dos controlos, permitem posteriormente criar "*Templates* de Indicadores" que fazem parte da automação subjacente ao *software*. Os parâmetros de conformidade permitem também criar "*Templates* de teste" para as entidades visto que a conformidade gere a comparação entre o cumprimento de regras durante os processos da empresa em relação aos requisitos reais em vigor.

Para obter um *template* de teste associa-se um tipo de entidade, ou as entidades individuais relevantes ao teste em si e ao resultado pretendido, a um objetivo de controlo. Após esta atribuição a faceta de automação do *software* encarrega-se de criar controlos automaticamente. A criação deste é feita com a lógica de um controlo por objetivo de controlo por entidade, ou seja, caso existam 50 documentos de autoridade, 50 objetivos de controlo, um por cada documento, e 50 entidades, irão ser criados um controlo por entidade, o que corresponde a cada um desses objetivos de controlo. O que ocorre nas "Operações Diárias" representadas na Figura 3.4, como resposta ao risco, é a monitorização dos controlos automaticamente criados pelo ServiceNow.

Como forma de medição da eficácia e respetivo nível de maturidade de conformidade, a automação do *software*, ao correlacionar os *templates* de indicadores e testes com os objetivos dos controlos, riscos e respetivas entidades, gera assistências que são atribuídas a colaboradores donos de entidades, de controlos ou donos de riscos. Estas, fornecidas regularmente à medida que os dados originais sofrem alterações de não conformidade, permitem a identificação momentânea de problemas de não conformidade.

Existe uma relação entre conformidade e risco pois a conformidade mitiga o risco, da mesma forma, ambos os módulos de risco e *policy & compliance* estão interligados onde o risco diário pode ser visto como compatível ou não com o risco residual alvo. Oposto ao risco, a política e a conformidade afetam diretamente a auditoria.

A auditoria interna é normalmente uma função de TI que olha para dois aspetos, ou seja, se os controlos que são executados são bem projetados e se são eficazes do ponto de vista operacional. O compromisso de auditoria é projetado especificamente para permitir testes seletivos dos controlos implementados que são monitorados, do ponto de vista da conformidade, sendo que, é feita uma análise tendo em conta a eficácia do projeto e eficácia operacional. Um controlo bem projetado é um controlo facilmente implementado e seguido. Deste modo, ao verificar a eficácia operacional dos mesmos, ou seja, quando os indivíduos responsáveis por estes realmente executam os seus processos diários de negócio, é possível averiguar o seu desempenho na mitigação dos riscos associados e na manutenção da conformidade dos processos. É aqui que a política e a conformidade afetam diretamente a auditoria e a apoiam, do ponto de vista de auditoria interna de TI, a "Revisão dos Controlos" através de "Tarefas de Auditoria" que, por sua vez, permitem também a automática "Geração de Problemas".

Neste módulo, a gestão de conformidade tem três etapas diferentes, primeiro, a documentação dos requisitos de órgãos reguladores externos, como governos federais, estaduais e locais, a UE ou outros órgãos internacionais e organizações da indústria, e agregação da lista de regras, regulamentos e melhores práticas obtidas. Em seguida é obtida a perspetiva dos donos de processos e operadores em relação à conformidade operacional com esses regulamentos e políticas por meio de controlos sobre os processos de negócios, dados e uma visão interna de como a empresa realmente cumpre normas e a aplicabilidade em como tal é atingido. Posteriormente é corrigido qualquer processo de negócios não compatível, se possível, e documentada a incapacidade de fazê-lo, se necessário. Caso os controlos indiquem que a organização está em incumprimento em relação a determinado assunto, o problema deve ser corrigido. Tal é feito via "Tarefas de Correção" pois, ao ocorrer, como resultado de um controlo, processos de negócios não compatíveis com requisitos definidos, o ServiceNow gera um problema automaticamente. Esse problema torna-se, então, o centro das tarefas de correção fornecendo, ao proprietário do controlo, a visibilidade das diferentes peças com necessidade de correção. Pode ser uma tarefa de correção simples em que, a título de exemplo, a equipa de desenvolvimento de aplicações deve alterar uma configuração ou executar um *patch*. Pode, no entanto, ser uma tarefa de correção complexa e ter vários pontos de retificação como, por exemplo, um problema que envolve o acesso a uma aplicação pela internet. Estes casos podem implicar que sejam envolvidas as equipas de desenvolvimento de aplicações, equipa de engenharia de rede, ou as equipas de engenharia dos servidores. Pode, ainda, ser desenvolvido um plano técnico de ação e mitigação usando uma estrutura de tarefa de remediação com encargos dependentes, um cronograma e diferentes grupos de atribuições, sendo elaborado um documento técnico, conforme a necessidade.

As estruturas de conformidade regulatória fornecem os controlos pelos quais as entidades são testadas. O ServiceNow disponibiliza dois métodos de avaliação de *compliance*.

O primeiro é um método subjetivo e é feito através de "*Attestations*" ou indicadores manuais. Esta forma de avaliação reúne as perspetivas de indivíduos com conhecimento direto dos processos de negócio em questão. As *attestations* ou indicadores manuais são obtidas através do envio de um questionário sobre o estado dos controlos pelos quais cada indivíduo é responsável. Se a conformidade for confirmada por esses indivíduos, é pedida uma evidência dessa verificação, embora não se qualifique tecnicamente como uma prova objetiva do ponto de vista de conformidade. O lado objetivo da avaliação, o segundo método de avaliação, é obtido através de indicadores automáticos, que pode ser algo tão simples como atribuir uma tarefa para fornecer dados de uma fonte externa ou tão complexo como uma consulta a várias tabelas do ServiceNow para identificar dados correlacionados que comprovam a conformidade. Usar consultas para pesquisar tabelas e usar código para identificar junções complexas de registos é executado pelo meio de indicadores objetivos que pesquisam automaticamente os dados existentes no ServiceNow.

O ServiceNow gera automaticamente problemas para controlos não compatíveis a partir dos quais a aceitação ou mitigação pode ser gerida. Se for aceite, espera-se que um registo de "Exceção de Política" seja criado, preenchido e enviado ao sistema. Se for mitigado, espera-se que uma tarefa de correção seja criada da mesma maneira. Na resolução de qualquer uma das hipóteses referidas, a expiração da exceção de política ou a conclusão da tarefa de correção, o controlo com falha deve ser reavaliado para provar que a conformidade foi alcançada.

Também neste módulo, a gestão de políticas, como perspetiva interna de como um regulamento externo ou melhores práticas se relacionam com a empresa, monitoriza o cumprimento das políticas. Quando relacionadas a controlos, as políticas agregam a conformidade a estes. As políticas são criadas, publicadas e geridas, são também publicadas como artigos de conhecimento na base de conhecimento de GRC.

4.
METODOLOGIA DA IMPLEMENTAÇÃO GRC

4.1. Enquadramento Prático

Para a correta implementação do projeto de gestão do risco na área de *Security&Risk* do Grupo EDP, formou-se uma equipa de colaboradores internos e externos ao Grupo EDP, nomeada a equipa GRC. A equipa GRC é composta por seis elementos, sendo que três são colaboradores internos e, os restantes, colaboradores externos pertencentes à empresa INTEGRITY.

A INTEGRITY é constituída por um conjunto de profissionais *experts* e seniores que conjugam uma elevada experiência com certificações internacionais relevantes em cada um dos seus sectores de atuação. É, portanto, uma empresa de consultoria e auditoria tecnológica com grande enfoque na segurança da informação. O objetivo da INTEGRITY é prestar serviços aos seus clientes de forma a que a sua informação esteja segura contra potenciais incidentes ou ataques de segurança (INTEGRITY, 2021).

Ainda, na prática de consultoria em cibersegurança, a empresa externa apoia os seus clientes na implementação e adoção de controlos com vista à redução efetiva do seu risco, nomeadamente, através da implementação de *standards* e *best practices* no que concerne à gestão da segurança de informação. Exemplos de Projetos Tipo que a INTEGRITY fornece são a "Certificação pelo Standard ISO 27001", a "Implementação de Métricas de Gestão de Segurança da Informação" e a "Seleção de Controlos Tecnológicos" (Consultoria em Cibersegurança | INTEGRITY, 2021).

A parceria entre as duas empresas, que forma assim a equipa GRC, reúne o conhecimento, formação e as capacidades necessárias à implementação da abordagem GRC, como é apresentado na Tabela 4.1 - Equipa GRC.

Tabela 4.1 - Equipa GRC

Equipa GRC		
Constituintes	Função/Responsabilidade	Experiência no Grupo EDP
Membro 1	Desenvolvimento da metodologia de implementação da abordagem GRC com a aplicação da metodologia FMEA e integração com o ciclo PDCA; Análise e implementação prática da metodologia desenvolvida e transição de dados para o *software* ServiceNow.	Estágio profissinal com duração de 7 meses e autora da presente dissertação.
Membro 2	Validação da metodologia desenvolvida; Análise sobre a situação atual e desenvolvimento dos objetivos do projeto; Configuração do *software* ServiceNow; Transição de dados para o *software* ServiceNow.	Colaborador do Grupo EDP, pertencente à DGU na área de *Security&Risk*.
Membro 3	Acompanhamento do projeto; Definição temporal de tarefas e atividades; Determinação de datas de entrega.	Colaborador do Grupo EDP, gestor de projetos.
Membro 4	Revisão documentacional; Identificação de princípios normativos.	*Compliance* na INTEGRITY.
Membro 5	Revisão documentacional; Identificação de princípios normativos.	*Compliance* na INTEGRITY.
Membro 6	Monitorização, correção e validação do trabalho de verificação documentacional.	*Compliance* na INTEGRITY.

Inicialmente a equipa GRC, de forma a garantir uma implementação da abordagem bem-sucedida, definiu os pontos a seguir mencionados como resposta às primeiras 4 etapas de implementação da abordagem GRC, como mencionado na Secção "3.3.3 Aplicação da Abordagem GRC", do Capítulo 3.

4.1.1. Definição de Objetivos

O objetivo deste protejo é dar respostas às limitações encontradas na gestão do risco em TI do Grupo EDP. Pretende-se, portanto, a concentração e centralização da informação TI e respetivos controlos e riscos numa plataforma apropriada e capacitada para tal.

Pretende-se, ainda, garantir a monitorização constante dos controlos implementados nos ativos correspondentes. Desta forma, ao correlacionar com os riscos existentes, é possível obter uma visão holística da posição momentânea da organização, a qualquer momento, considerando todas as vulnerabilidades que existem, como estão a ser tratadas, controladas ou aceites, e o estado de *compliance* regulamentar da empresa.

Foram ainda definidas metas de processo que se encontram distribuídas temporalmente na Figura 4.1.

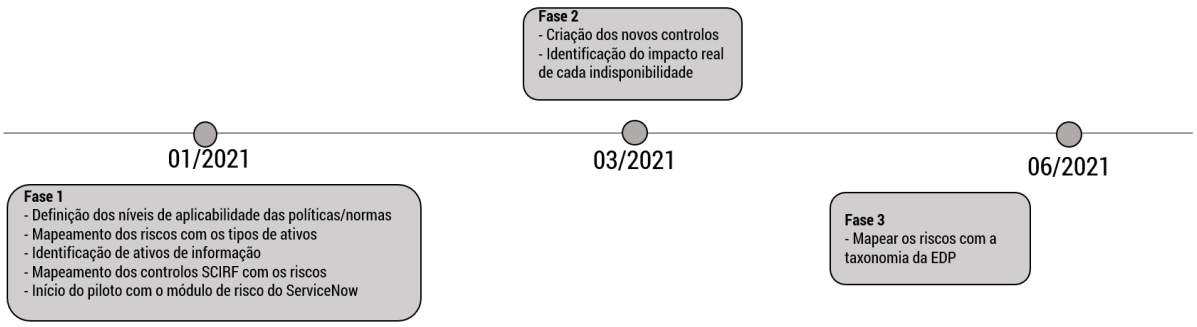


Figura 4.1 - Distribuição temporal das metas da abordagem GRC

Após a última data referida no espectro da Figura 4.1, ou seja, junho de 2021, continuar-se-á o trabalho de população de informação do *software* ServiceNow com todos os dados até à data trabalhados, analisados e transformados. Tal procedimento é feito em massa, sendo que, após esta população de dados a grande escala, existe trabalho contínuo de atualização e melhoria da automatização. É, portanto, um projeto ilimitado no tempo, posteriormente a todo o trabalho intensivo de configuração, procura e associação de informação, visto que a legislação será sempre atualizada e alterada e os próprios riscos e resultados de controlos implementados na organização são agora monitorizados em tempo real.

4.1.2. Análise da Situação Atual

Neste ponto a equipa recolheu informação sobre o estado atual, em termos de *governance*, risco e *compliance*, do Grupo EDP. A recolha da informação pretinente teve em conta uma análise do funcionamento interno dos processos da empresa, uma revisão de toda a regulamentação interna e ainda consideração sobre os conhecimentos de diversos colaboradores de outros departamentos.

Em termos de *governance*, a situação atual apresenta o apropriado processo de construção, manutenção e aprovação de requisitos legais, sendo que, os documentos que enunciam a regras de trabalho e segurança do Grupo estão hierarquizados e a respetiva aprovação é feita tendo em conta o grau de criticidade do documento em si. No entanto, ocorre a inexistência de controlo e monitorização referente à aplicação e implementação das regras e leis normativas. Encontram-se, portanto, documentadas as boas práticas que devem reger o funcionamento da empresa ainda que a execução das mesmas não se encontre supervisionado nem evidenciado regularmente visto que, apenas em contexto de auditoria, tais regras e boas práticas são questionadas e pedidas evidências de conformidade operacional das mesmas.

Em termos de risco, confirma-se que os controlos existentes e presentemente em funcionamento estão distribuídos pelas áreas sem conformidade ou interligação entre si e com os normativos. Os controlos necessários à segurança da informação existem e são monitorizados. No entanto, a associação ao risco não está regularizada igualmente em toda a organização visto que cada área trata o tema de forma individual e personalizada, dificultando, assim, a auditoria do Grupo como um todo e a uniformização dos princípios de segurança.

Acrescenta-se ainda que a avaliação do risco é feita de forma qualitativa, instintiva e de acordo com a experiência dos colaboradores. Tal fator pode influenciar o nível do risco real

pois as perspetivas, quando comparadas, podem não ser coesas. Devido a tal, a abordagem GRC vem revolucionar este critério de avaliação qualitativa ao inserir valores financeiros relacionados com os diferentes níveis de impacto e espectros temporais definidos relacionados com os diferentes níveis de probabilidade. Desta forma, a escolha e a avaliação do grau de risco final que certa vulnerabilidade ou falha apresenta para o Grupo EDP, tem por base elementos reais e comparáveis, permitindo assim uma noção realista e conforme entre todos.

Em termos de *compliance*, a informação recolhida indica a existência de cerca de 50 documentos de legislação e/ou boas práticas, incluindo políticas, normas, especificações de trabalho, manuais e instruções. A documentação é considerada, pela equipa, conforme, tendo em conta que a base da mesma assenta na estruturação proposta pela ISO/IEC 27001:2013.

4.1.2.1. Estruturação da Documentação EDP

Toda a documentação interna do Grupo é baseada nos princípios e controlos da ISO/IEC 27001:2013. Os controlos mencionados na ISO em questão estão distribuídos como apresentado na Figura 4.2.

Figura 4.2 - Estruturação dos controlos da ISO/IEC 27001:2013

A ISO/IEC 27001:2013 inclui 11 áreas de controlo sendo, na empresa em questão, a base para as diversas normas e políticas. Nomeadamente, estas áreas incluem a: Política de Segurança, Organização da Segurança da Informação, Gestão de Ativos, Segurança dos Recursos Humanos, Segurança Física e Ambiental, Gestão de Comunicações e Operações, Controlo de Acesso, Aquisição de Sistemas de Informação, Desenvolvimento e Manutenção, Gestão de Incidentes de Segurança da Informação, Gestão da Continuidade das Empresas e Conformidade. Esta norma é a base de avaliação e auditoria para a criação, implementação e manutenção do Information Security Management System (ISMS). Vários organismos de certificação

em todo o mundo são acreditados por organismos nacionais para auditar o cumprimento da ISO/IEC 27001:2013 e emitir certificados para organizações de participantes (Li et al., 2015).

Este sistema de gestão de segurança da informação adotado pelo Grupo EDP preserva a confidencialidade, integridade e disponibilidade da informação, aplicando um processo de gestão do risco que oferece confiança às partes interessadas de que os riscos são geridos de forma adequada. É importante que o sistema de gestão de segurança da informação faça parte e esteja integrado com os processos da organização e estrutura geral de gestão. Ainda é de destacar que a segurança da informação seja considerada no desenho de processos, sistemas de informação e controlos.

Esta norma internacional especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto de uma organização. Também inclui requisitos para a avaliação e tratamento dos riscos de segurança da informação adaptados às necessidades da organização. Os requisitos estabelecidos neste documento são genéricos e aplicáveis a todas as organizações, independentemente de tipo, tamanho ou natureza. De forma a manter a conformidade com a legislação, na EDP, são documentadas normas e políticas correspondentes a cada uma das 11 áreas de controlos da ISO/IEC 27001:2013. Ainda a estas são acrescentadas políticas e normas mais específicas às necessidades da organização, sendo que, os documentos analisados na metodologia de implementação da abordagem GRC incindem em 13 normas internas, 10 políticas internas e uma ordem de serviço.

4.1.3. Definição do Ponto de Partida

A implementação da abordagem GRC ocorre por áreas ou unidades de negócio do Grupo EDP. No caso concreto da presente dissertação, esta implementação assenta numa primeira iteração deste projeto relativa aos riscos operacionais que ocorrem, ou podem ocorrer, na área de segurança em TI da organização, mais precisamente na unidade DGU. Pretende-se, após esta primeira implementação, a expansão da metodologia GRC desenvolvida para as restantes unidades do Grupo. Tal expansão será, assim, facilitada pois é assente num *upgrade* em massa dos dados existentes relativos a outras áreas, visto que a configuração e *design* da estrutura do processo de implementação já estará decidido e tratado.

4.1.4. Monitorização

De forma a controlar todo o desenvolvimento do projeto e monitorizar as metas definidas por fases na Figura 4.1, são calendarizadas reuniões semanais internas com os elementos internos da equipa. Nestas é feito um ponto de situação dos progressos atingidos na semana de trabalho assim como a resolução das dificuldades encontradas e um acerto dos objetivos de trabalho para a seguinte reunião. Ainda nestas reuniões de equipa interna são efetivadas comunicações com a equipa do *software* ServiceNow caso haja necessidades de novas configurações ou correções das configurações já existentes no *software*.

Acrescenta-se como forma de monitorização da metodologia de implementação da abordagem GRC, aplicada até à fase 2, ou seja, nos primeiros 3 meses do projeto, reuniões

quinzenais com os elementos externos da equipa GRC. A equipa INTEGRITY é responsável pela análise da documentação interna do Grupo EDP com o objetivo de definir os níveis de aplicabilidades das regras definidas nas políticas e normas internas assim como enumerar os princípios descritos nas mesmas. Em conjunto e com a totalidade da equipa GRC, é feito o trabalho de associação entre os princípios identificados e os possíveis riscos que o não cumprimento dos mesmos pode levantar. Nestas reuniões é então efetuada, também, uma atualização por parte de todos os membros do trabalho até ao dia realizado, esclarecimento de dúvidas e debate conjunto dos principais riscos adjacentes.

Por fim ocorre o reporte ao chefe da equipa de segurança da unidade DGU. Este reporte é feito ao longo de reuniões quinzenais e é presenciado pelos elementos internos da equipa GRC. Este é o momento de apresentação de resultados e resumo da situação atual do projeto. Após a exposição do estado da abordagem GRC é feita uma reflexão conjunta das melhorias que podem ser aplicadas às quais são acrescentadas as sugestões e críticas construtivas adquiridas por parte do chefe da equipa de segurança.

4.1.5. Road Map

Em acrescento a todas as estratégias definidas pela equipa GRC, idealizou-se ainda um *road map* dos vários níveis do processo de gestão do risco e segurança em TI ao longo dos anos, na unidade DGU. O mesmo encontra-se na Figura 4.3.

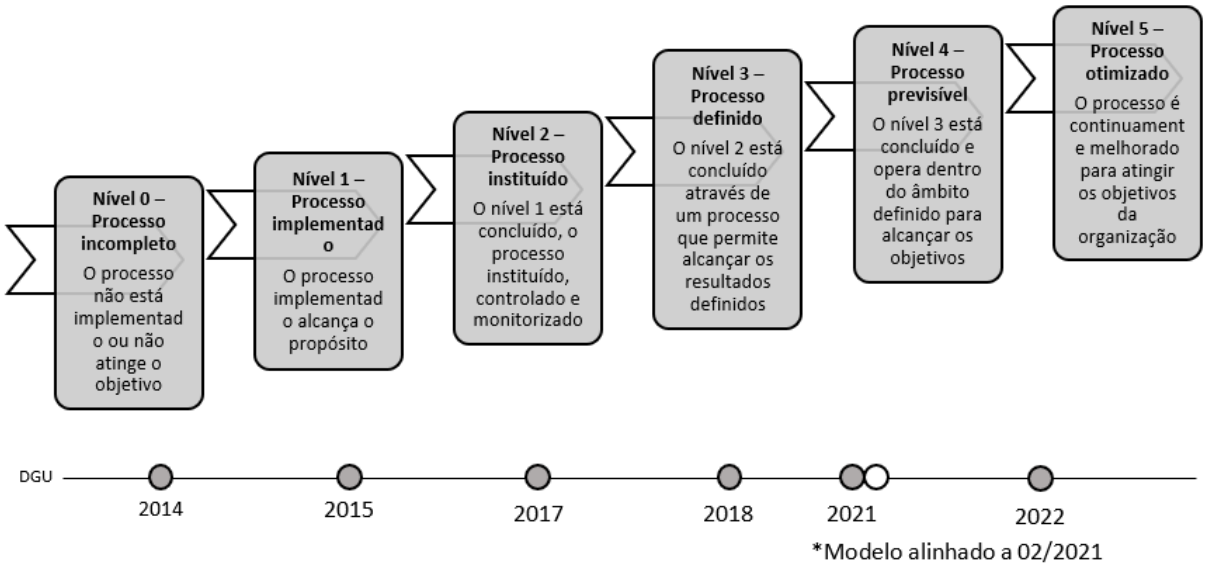


Figura 4.3 - Road map da abordagem GRC

Como é possível observar na Figura 4.3, a DGU já completou o nível 3 do processo e completa o próximo nível de maturidade através da implementação da monitorização do risco e *assessments* internos, ou seja, através da completa implementação da abordagem GRC. A gestão do risco em TI torna-se um processo otimizado quando a abordagem GRC estiver conforme e integrada nas atividades operacionais, sendo que, desse momento para a frente, existirá apenas processos de melhoria contínua.

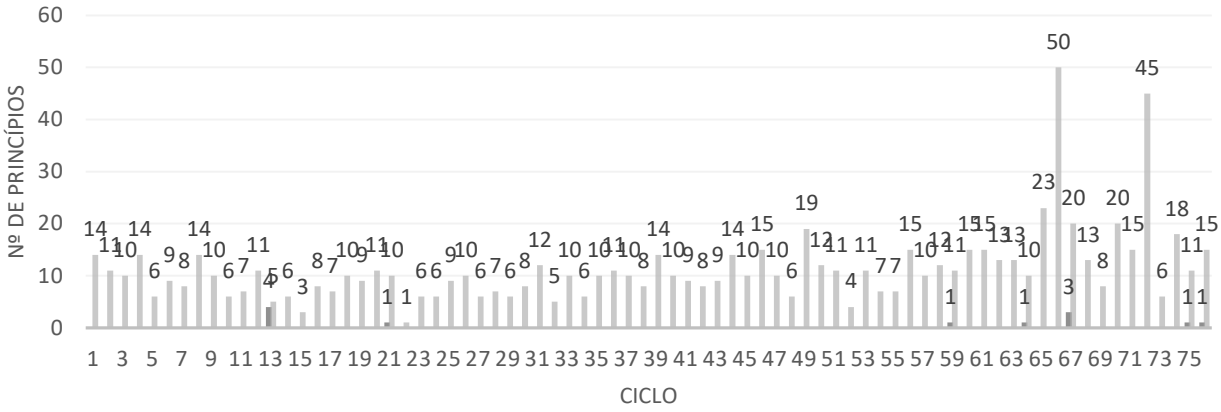
4.2. Plano de Implementação GRC

Em seguida apresenta-se o plano de implementação do projeto de gestão do risco TI segundo a abordagem GRC. Este decorre segundo a Figura 4.4 abaixo e é colocado em prática ao longo da descrição referida no Capítulo 5. O plano em referência foi desenvolvido préviamente pelo Grupo EDP em atividades de conceção da implementação da abordagem GRC. Devido a tal é considerado como um plano intemporal visto que novas normas ou polícas surgem regularmente, consequentemente, novos princípios e até mesmo nosvos ativos de informação irão também surgir no decorrer dos anos.

Segundo o plano PDCA implementado, os princípios são extraídos da documentação existente no Grupo EDP, a qual apresenta regras essenciais e cujo cumprimento favorece o correto funcionamento da empresa, evitando assim potenciais falhas. O incumprimento de cada princípio descrito numa política ou norma, dá, assim, origem a um potencial modo de falha que, por sua vez, tem efeitos de risco. Cada efeito de uma potencial falha é um possível risco e a este estão associados um ou mais controlos que permitem medir a exposição ao risco. É, desta forma, elaborado não só um catálogo de risco como também um catálogo de controlos. A efetividade dos controlos é, ainda, verificada e monitorizada regularmente sendo que, em caso de necessidade, são tomadas medidas de melhoria e correção de controlos deficientes.

Figura 4.4 - Plano de implementação da abordagem GRC

Toda a análise e inserção de dados segundo o plano PDCA desenhado ocorre um total de 76 vezes em ciclos de 10 princípios, em média, como representado no Figura 4.5.



Como ferramenta de suporte à implementação da abordagem GRC recorre-se à metodologia FMEA e aos seus princípios. A aplicação da metodologia FMEA encontra-se relacionada com o plano PDCA referido. Existe, portanto, a subdivisão da informação necessária pelas fases do plano criado para este trabalho. Desta forma, é possível verificar o estado dos dados recolhidos segundo as fases "PLAN", "DO", "CHECK" e "ACT". Estas são ainda seguidas, segundo a metodologia FMEA, pela última secção de "Resultados" onde é possível confirmar a efetividade das ações de melhoria e correção selecionadas e implementadas. Note-se, ainda, que é adicionada uma coluna na fase "DO" remetente para os tipos de ativos relacionados com o potencial modo de falha em questão, tal acrescento foi adicionado de forma a facilitar a transição dos dados recolhidos para o *software* ServiceNow visto que há a necessidade de relacionar com entidades.

É possível observar esta adequação e forma como está estruturada e organizada a análise e recolha de dados na Tabela 4.2.

Tabela 4.2 - Estruturação da metodologia FMEA

PLAN		DO									CHECK	ACT		Resultados			
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos	Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
Função	Potenciais Modos de Falha					Prev.	Det.										

É de notar que o tipo de metodologia FMEA escolhida para a implementação prática da metodologia desenvolvida pela autora da presente dissertação teve em conta o conhecimento adquirido pela investigação literária. Devido a tal, por motivos de adequação ao pretendido pelo Grupo EDP e ao tipo de projeto em si, é colocada em prática o tipo de metodologia FMEA de processo.

Primeiramente, através da análise da documentação, são identificadas, assim, as potenciais falhas do incumprimento das regras legisladas, fase "PLAN". Nesta primeira fase de recolha de dados, são consideradas Potenciais Modos de Falha qualquer incumprimento das regras estabelecidas nas normas, políticas, etc.

Desta recolha são, então, analisados os potenciais riscos ou efeitos da realização desses mesmos Potenciais Modos de Falha documentados e as respetivas causas, tal ocorre na fase "DO". É importante realçar a diferença na excução deste parâmetro do ciclo PDCA perante a metodologia teórica, visto que esta colocaria a análise de efeitos e causas na fase anterior do ciclo. A diferença de execução ocorre devido a motivos internos ao Grupo EDP assentes na facilidade de processar e guiar metodicamente o trabalho que ocorre neste campo, de forma a permitir a separação e simultaneidade de atividades entre os membros da equipa GRC.

Os potenciais efeitos das falhas e mecanismos de falha ou causas são sistematizados através de um *brainstorm*, onde, pelo conhecimento de funcionamento da organização, é possível prever consequências e causas não favoráveis, sendo que estes não se encontram documentados como normativos e seguem apenas o instinto da experiência. Ocorre diversas vezes que várias falhas potenciais agregam-se num só risco ou efeito. Ainda associadas a estas e ainda na fase "DO", são estabelecidos os controlos, alguns destes descritos nas regras em si e outros interligados com controlos já existentes na organização. Esta interligação é de grande relevância para a segurança do Grupo assim como para efeito de auditorias externas ou internas, pois, deste modo, é possível substanciar a importância dos controlos em ação, responder a questões de origem, motivo, importância e efeito real dos mesmos.

É ainda importante referir que para cada potencial falha podem ser estabelecidos vários controlos, estes podem ainda multiplicar-se tendo em conta o número de ativos que afetam, esta situação ocorre relativamente aos controlos que não são baseados na definição de procedimentos e regras. Toda a relação com os ativos mencionada é feita recorrendo ao *software* ServiceNow, a associação entre controlos e respetivos ativos é simplificada com a utilização deste *software* pois permite a escalabilidade desta abordagem a todos os ativos existentes na empresa de forma simples, prática e rápida.

Ainda na fase "DO" é feito o processo de avaliação do impacto e probabilidade dos potenciais efeitos e causas das falhas identificadas na fase anterior assim como a avaliação, em termos de deteção, dos controlos associados. Todo o processo de avaliação ocorre no *software* ServiceNow onde os colaboradores responsáveis pelas potenciais falhas e controlos correspondentes dão resposta a uma assistência ao risco enviada automaticamente. Esta assistência ao risco pretende obter como resultado os pontos de avaliação da FMEA de forma a preencher a metodologia FMEA na secção "DO" e a possibilitar o cálculo do grau de risco antes da confirmação e teste da efetividade dos controlos e possíveis ações de melhoria ou correção necessárias.

Em seguida, na fase "CHECK", recorrendo, mais uma vez, ao *software* ServiceNow, é testada a efetividade dos controlos estabelecidos. Esta monitorização é feita automaticamente, nos casos em que é possível, e manualmente, onde, os donos dos controlos evidenciam a efetividades dos controlos pelos quais estão responsáveis através do preenchimento de uma questionário e anexo de evidências de conformidade. A monitorização no *software* recorre a

indicadores ou a *asssements* dos próprios controlos, dependendo do potencial modo de falha em questão, e traduz o resultado dos mesmos em percentagem de *compliance*, como é demonstrado no decorrer no Capítulo 5.

Quando a existência de falhas ou controlos não compatíveis, o *software* gera automaticamente problemas, tal ocorre na fase "ACT" do PDCA desenvolvido. Dos problemas identificados, os colaboradores responsáveis pelo controlo ineficiente podem aceitar o problema ou implementar melhorias e corrigir os defeitos do mesmo através de tarefas de correção.

Por fim, o ServiceNow permite calcular os novos parâmetros de avaliação do risco em comparação com os resultados obtidos antes da implementação de qualquer ação de melhoria contínua. Na última fase do plano PDCA recorre-se, novamente, a uma reavaliação dos parâmetros iniciais. Esta ocorre no *software*, no entanto, é feita unicamente automaticamente sem a perceção dos colaboradores, como o caso da avaliação primária destes mesmos valores. Estes encontram-se, assim, calculados automaticamente tendo em conta a percentagem de *compliance* dos controlos, ou seja, a sua efetividade, atribuídos às potenciais falhas, incluindo ainda a contabilização de quaisquer ações de melhoria e correção aplicadas, sendo, por isso, possível preencher a última secção da FMEA, secção dos "Resultados".

5. CASO DE ESTUDO: GRUPO EDP

O Grupo EDP é uma empresa multinacional de serviços públicos verticalmente integrada. Ao longo de mais de 40 anos de história, tem vindo a construir uma presença relevante no cenário energético mundial, estando presente em 22 países, em 4 continentes.

Com mais de 12.100 colaboradores, o Grupo está presente em toda a cadeia de valor da eletricidade e na atividade de comercialização de gás. A empresa é considerada a quarta maior produtora de energia eólica do mundo e 74% da energia é produzida a partir de recursos renováveis. A EDP - Energias de Portugal fornece, assim, eletricidade e gás a mais de 9 milhões de clientes.

O Grupo aderiu à Euronext Lisbon em 1997 e tanto a EDP Brasil como a EDP Renováveis são também empresas cotadas. A sustentabilidade faz parte do ADN da empresa e esta é, ainda, membro do Índice Dow Jones de Sustentabilidade.

5.1. Gestão do Risco no Grupo EDP

No que se refere à estrutura organizacional da gestão do risco na empresa, o Conselho de Administração Executivo (CAE) é apoiado pela Direção de Gestão do Risco (DGR) e pelo Comité de Risco. Existe ainda uma estrutura matricial de coordenação funcional entre a DGR e os *Risk Officers* das Unidades de Negócio que dispõem dessa estrutura (EDP, 2021).

Cabe ao CAE a aprovação das políticas de risco, a definição das estruturas de acompanhamento e a aprovação dos limites de risco a estabelecer.

O Comité de Risco reúne regularmente e é integrado por membros dos Conselhos de Administração ou representantes de diversas empresas do Grupo e ainda por diretores corporativos, nomeadamente o Diretor da Gestão do Risco.

Compete ao Comité de Risco monitorizar os riscos significativos e o perfil de risco do Grupo EDP, aprovar o modelo de relatórios periódicos a apresentar pelas unidades de negócio ou pela Direção de Gestão do Risco, bem como o de outros mecanismos de reporte e monitorização dos riscos da EDP. É ainda responsável por aprovar ou definir recomendações sobre riscos significativos do Grupo EDP e sobre situações extraordinárias em termos de risco para apreciação pelo CAE, emitir recomendações sobre políticas, procedimentos e limites de risco para o Grupo EDP, para apreciação e aprovação pelo CAE (EDP, 2021).

No âmbito da Política Corporativa de Gestão Empresarial de Risco da EDP é exigido que todos os riscos relevantes sejam identificados e geridos, e clarificado em que empresas está localizada a sua gestão, bem como a cadeia de responsabilidades envolvida.

Como ferramenta de suporte ao *risk assessment*, é utilizado o Portal de Risco EDP, aplicação informática que concentra informação relativa à identificação, análise, avaliação, medidas de mitigação e monitorização de riscos relevantes relacionados com as atividades do Grupo EDP, para além de permitir a sua divulgação transversal no seu universo de empresas. Desta forma facilita-se o *benchmarking* dos riscos e da respetiva gestão e controlo em áreas homólogas das empresas do grupo, o que permite a partilha de *best practices* («Fatores de Risco», 2021; Gestão de Risco, 2021).

O Portal de Risco EDP, atualizado periodicamente pelos responsáveis dos riscos, é consultável por colaboradores autorizados, nomeadamente a Alta Direção, constituída por administradores executivos e diretores centrais das *holdings* e *sub-holdings*, possibilitando o conhecimento, de forma expedita, de riscos relevantes do Grupo EDP e de cada empresa em cada momento, o seu impacto e o modo como está a ser processada a sua gestão e controlo e as melhorias em curso neste domínio (EDP, 2021).

5.1.1. Tipos de Risco no Grupo EDP

Os riscos a que está exposto o Grupo EDP são os típicos das *utilities* de eletricidade e gás, designadamente:

- Riscos de Negócio: relativos ao crescimento sustentável da atividade, nomeadamente no equilíbrio entre energia e ambiente por meio da promoção da eficiência dos consumos, de soluções de redes inteligentes e da descarbonização da produção da eletricidade, inclui, ainda, o risco regulatório;
- Riscos de Mercado: relacionados com preços e volumes de eletricidade e outras *commodities*, taxas de câmbios e de juro;
- Riscos Operacionais: este é o grupo com a maior diversidade, englobando desde equipamentos e processos a falhas humanas, sem esquecer outras matérias como a prevenção, segurança e o risco legal;
- Riscos de Crédito: neste grupo incluem-se os riscos de incumprimento de clientes e de contrapartes.

5.1.2. Metodologia de Gestão do Risco no Grupo EDP

A avaliação integrada do nível de risco do Grupo EDP é feita por meio do modelo de análise *bottom up* designado por "Cash Flow at Risk", o qual permite a avaliação da incerteza associada ao valor de EBITDA (Earnings before Interest, Taxes, Depreciation and Amortization), ou outra grandeza, como por exemplo o FCF (Free Cash Flow) at Risk, bem como da eficácia das estratégias de *hedging* adotadas, estas assentam em estratégias de proteção para riscos de um investimento cujo objetivo é eliminar ou minimizar a possibilidade de perdas futuras (EDP, 2021).

Complementarmente é utilizado um modelo *top down* que se baseia na evolução das cotações das ações e na previsão dos valores de "beta" de cada unidade de negócio, o qual

visa a determinação do risco associado aos ativos e ao capital próprio, como ainda a comparação com outras empresas do sector (EDP, 2021).

Também a gestão do risco em TI do Grupo EDP segue os processos neste ponto descritos. Faz uso, ainda, de uma tecnologia de monitorização de eventos relativos aos riscos de TI, sendo esta o sistema SIEM. A implementação da abordagem GRC vai comaltar as insuficiencias encontradas no sistema atual de gestão de risco em TI. Mais precisamente, pretende corrigir a falta de ligação com fatores de conformidade, a inexistência de uma centralização de *risk data* e a desatualização da informação sobre o estado atual da empresa em termos de risco e compatibilidade legal.

O caso prático da efetivação da metodologia de implementação da abordagem GRC é pormenorizado nos restantes pontos do presente capítulo. Tal caracterização é feita seguindo a lógica do plano PDCA desenvolvido no Capítulo 4, na Secção "4.2 Plano de Implementação GRC".

5.2. PLAN

O início da implementação de toda a abordagem GRC inicia-se com a fase “PLAN” do ciclo PDCA desenvolvido. Esta assenta na análise de toda a documentação que gere as regras legislativas do Grupo EDP. Os documentos analisados incluem normas e políticas de boa conduta, as quais, sendo corretamente implementadas e monitorizadas, fornecem uma gestão contra falhas e respetivos efeitos potenciais.

Para efeitos demonstrativos da presente dissertação e proteção da privacidade do Grupo EDP, é feita a análise da Norma de Controlos de Acessos do Grupo EDP, uma das normas analisadas e na qual o presente trabalho é baseado. No entanto, a mesma linha de raciocínio e processo apresentado neste documento é transcrito para as restantes normas e políticas da organização.

São, portanto, analisadas no decorrer da implementação da abordagem GRC de gestão do risco em TI vários documentos normativos, entre eles, 1 ordem de serviço, 10 políticas e 13 normas. A hierarquização dos documentos normativos do Grupo EDP encontra-se representada no esquema em pirâmide da Figura 5.1.

Figura 5.1 - Hierarquização normativa do Grupo EDP

5.2.1. Norma Controlo de Acessos

O objetivo desta norma é estabelecer os princípios e as melhores práticas de segurança da informação a aplicar na gestão das contas de utilizadores e acessos aos sistemas de informação do Grupo EDP e outros recursos TI, quando aplicável.

Esta norma é a base para a implementação de um processo adequado e controlado de gestão do ciclo de vida dos utilizadores, de forma a assegurar que apenas os utilizadores autorizados têm acesso aos sistemas do Grupo EDP, e que os acessos atribuídos estão de acordo com as suas funções.

A aplicação dos princípios enumerados neste documento não inviabiliza a utilização de medidas complementares de segurança nos acessos lógicos, definidas pelas entidades competentes. Esta norma está aprovada, tendo sido criada em alinhamento com a Política de Segurança de Informação e com a legislação e regulamentação vigente.

Esta norma e os princípios aqui definidos são, ainda, aplicáveis a todos os colaboradores do Grupo EDP e entidades externas que possuam uma conta de utilizador para acesso a qualquer sistema ou recurso de TI do Grupo EDP, e/ou que tenham responsabilidade na gestão das contas e acessos de utilizadores. Exceto se explicitamente referido o contrário, os princípios enumerados nesta norma são também aplicáveis à totalidade dos sistemas e recursos de TI do Grupo EDP.

Cada utilizador é responsável por gerir as suas contas de acesso aos sistemas e recursos de TI do Grupo EDP de acordo com esta norma. Adicionalmente, todos os utilizadores são responsáveis por reportar qualquer violação detetada dos princípios aqui definidos. Os princípios estabelecidos nesta norma devem ser, por isso, comunicados, aceites e respeitados por todos aqueles a quem esta se aplica.

A DGU, através da área de Security & Risk, é responsável por definir as regras para a gestão das contas e acessos dos utilizadores aos sistemas do Grupo EDP, e pelo sistema de gestão de identidades e acessos.

As áreas responsáveis pela gestão dos sistemas ou recursos de TI, incluindo, mas não se limitando à DGU, e que são responsáveis pela implementação e gestão das configurações técnicas e de segurança da informação nos sistemas, devem seguir e implementar os princípios e regras definidas nesta norma.

5.2.2. Implementação na Metodologia FMEA

O preenchimento do início da metodologia FMEA efetua-se ao indicar a função das regras descritas no normativo aplicável. A função tem, portanto, em consideração o objetivo do documento normativo e é preenchida na secção de identificação, primeira coluna. Para o caso considerado, relativamente à Norma de Controlo de Acessos, esta célula é preenchida com a função "Controlar Acessos", como indicado na Tabela 5.1.

Ainda nesta secção, na coluna "Potenciais Modos de Falha", encontra-se descrito a falha ocorrente do não cumprimento das regras mencionadas no documento selecionado na coluna função. As primeiras duas regras ou princípios encontrados na norma em questão encontram-se descritos na secção "Princípios gerais" do normativo. Esta secção refere o seguinte:

4.2 Princípios gerais

O acesso à informação, aos sistemas e recursos de TI do grupo EDP, e aos seus processos de negócio é controlado com base nos requisitos de segurança da informação e de negócio, bem como nos requisitos de legislação e regulamentação. O acesso aos sistemas e aplicações é restringido aos utilizadores autorizados, garantindo a utilização de mecanismos de autenticação adequados e registando os acessos realizados.

Nos anexos é possível observar toda a listagem dos potenciais modos de falha identificados nesta norma.

A Tabela 5.1 apresenta, ainda, as duas regras transcritas da Norma Controlo de Acessos transformadas em potenciais modos de falha, ou seja, é descrita a potencial falha consequente do não cumprimento das regras transcritas, neste caso, referentes à secção "Princípios gerais".

Tabela 5.1 - FMEA exemplo fase "PLAN"

PLAN	
Identificação	
Função	Potenciais Modos de Falha
Controlar Acessos	O acesso à informação, aos sistemas e recursos de TI do Grupo EDP, e aos seus processos de Negócio não é controlado com base nos requisitos de Segurança da Informação e de Negócio, bem como nos requisitos de legislação e regulamentação
	O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados

O restante preenchimento da metodologia FMEA encontra-se, também, nos anexos desta dissertação.

5.2.3. Implementação no *Software* ServiceNow

Para implementar a fase "PLAN" no *software* ServiceNow, foram inseridas todas as políticas e normas trabalhadas pela equipa GRC. Tal atividade foi feita no módulo *policy & compliance* do *software* como apresenta a Figura 5.2, é possível ainda identificar na terceira linha a norma em trabalho no presente documento.

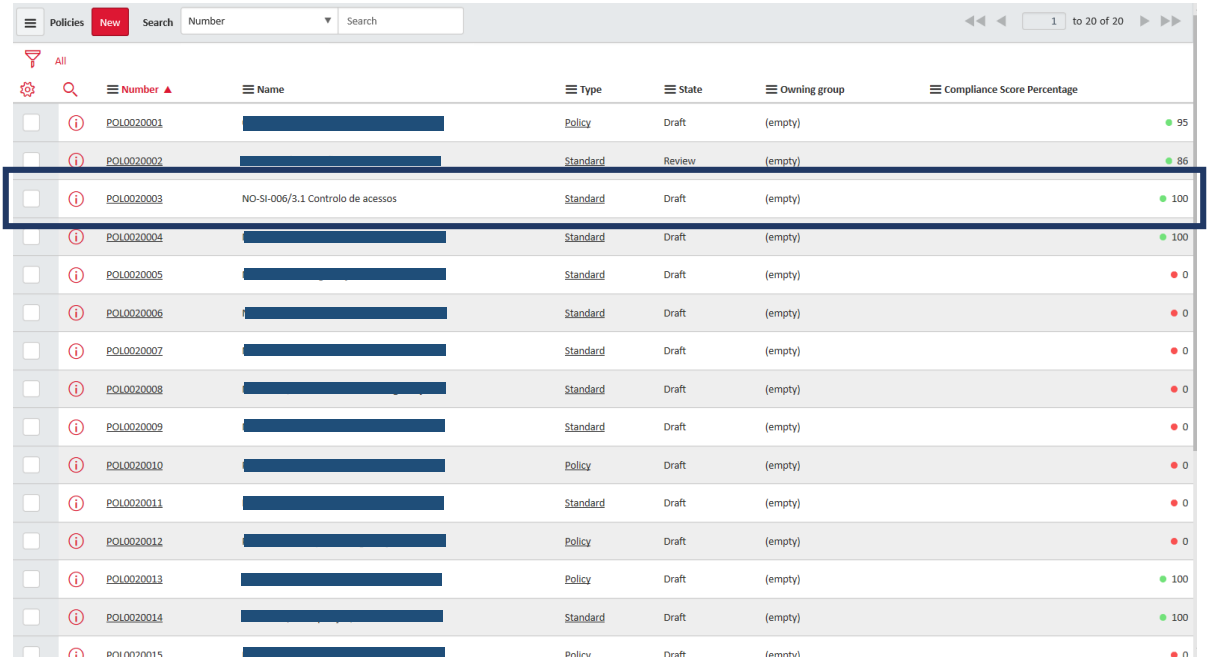


Figura 5.2 - Documentação no ServiceNow

Ao selecionar a Norma de Controlo de Acessos, é aberta uma página mais detalhada sobre a mesma como se encontra exposto da Figura 5.3.

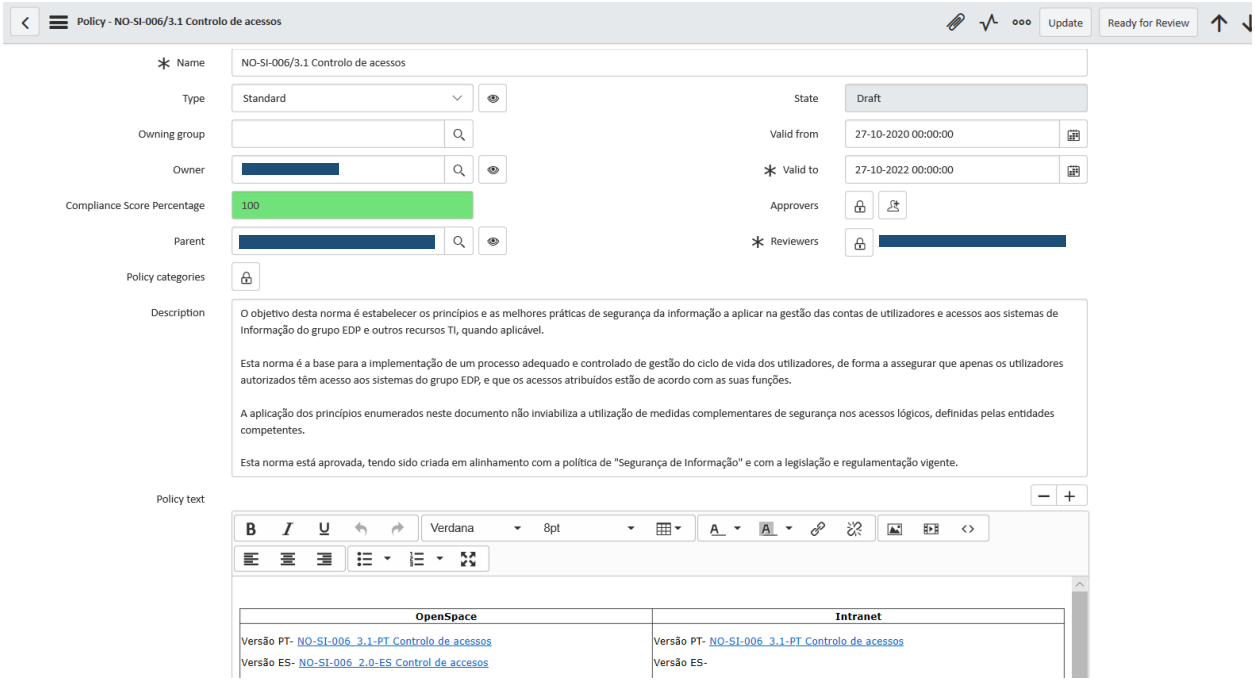


Figura 5.3 - Norma Controlo de Acessos no ServiceNow

Neste campo do *software* é feita uma breve referência ao normativo e descrição do mesmo. É, ainda, possível identificar o responsável pelo normativo, os revisores deste e o documento normativo sobre o qual este teve origem, ou seja, o normativo "pai", que é a ordem de serviço do Grupo EDP, como indicado na área "Parent". Acrescenta-se ainda a possibilidade de identificar a validade do documento, geralmente os normativos da organização tem uma duração de 2 anos, desta forma, uma notificação automática é enviada para o responsável perto do fim do prazo com a necessidade de revisão da norma.

A equipa GRC decidiu ainda, em vez de transcrever o texto do documento na íntegra para o preenchimento da área "Policy text", construir uma tabela com os diversos *links* onde o documento pode ser encontrado e analisado, assim como as respetivas traduções. Tal decisão foi tomada tendo em consideração a dimensão do Grupo EDP e restrições de acessos a sites de partilha de informação interna, como o "OpenSpace" e a "Intranet", e a geografia da empresa, sendo que existem colaboradores de diversas nacionalidades.

Na seguinte fase do plano PDCA é feita a ligação dos riscos decorrentes dos potenciais efeitos de falha e controlos encontrados às diversas normas e políticas mencionadas neste campo do *software* ServiceNow.

5.3. DO

Na secção "DO" do plano PDCA desenvolvido pela equipa GRC mencionam-se os possíveis efeitos e causas da respetiva falha potencial assim como os ativos atingidos pela mesma e os controlos considerados necessários à monitorização desta.

Este procedimento efetua-se com a totalidade da equipa GRC onde, um processo de *brainstorming*, experiência e intuição é posto em prática. Em conjunto, são debatidos individualmente os potenciais modos de falha com o objetivo de preencher a metodologia FMEA de acordo com a realidade diária do Grupo EDP.

5.3.1. Implementação da Metodologia FMEA

No seguimento do exemplo mencionado na secção "PLAN", são analisados quais os potenciais efeitos de ambas as falhas referidas na Norma Controlo de Acessos.

São, portanto, identificadas as causas que podem levar à materialização da falha, são ainda definidos os controlos relacionados com a falha em questão e identificados quais os ativos afetados pela mesma como demonstra a Tabela 5.2, sendo esta a continuação do preenchimento da tabela anterior.

Tabela 5.2 - FMEA exemplo fase "DO"

PLAN		DO								
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos
Função	Potenciais Modos de Falha					Prev.	Det.			
Controlar Acessos	O acesso à informação, aos sistemas e recursos de TI do Grupo EDP, e aos seus processos de Negócio não é controlado com base nos requisitos de Segurança da Informação e de Negócio, bem como nos requisitos de legislação e regulamentação	Acesso ilegítimo	**1**	Existência de controlos de acesso ineficientes devido a incoerências com a legislação	**2**	Procedimentar a articulação com a área de Segurança de Informação do Grupo EDP Procedimentar o controlo de acesso à informação	-	**5**	**10**	*Governance*
	O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados	Acesso ilegítimo	**3**	Acesso ilegítimo por incorreta restrição de utilizadores	**1**	-	Sistema de deteção de credenciais inexistentes Autenticação	**1**	**3**	Aplicações CMDB

Acrescenta-se ainda a avaliação da gravidade e ocorrência das potenciais falhas assim como a deteção dos controlos mencionados na metodologia FMEA, e, transcritos em massa para o *software* ServiceNow. Esta avaliação é assente não só em debates conjuntos entre a equipa GRC e diversos responsáveis de monitorização de todas as áreas que compõem a DGU como também segundo a opinião e experiência dos colaboradores responsáveis pelas diversas potenciais falhas ou entidades relacionadas com estas.

Tanto para a gravidade como para a probabilidade de ocorrência, os valores quantitativos, para o impacto os valores financeiros e para a probabilidade os valores estatísticos de percentagem, continuam presentes mesmo tento em conta uma avaliação final qualitativa, estes podem ser encontrados nas Tabelas 5.3 e 5.4. Note-se que os valores apresentados têm por base informação *standard* por motivos de confidencialidade e proteção dos dados do Grupo EDP. Ainda, a escala da avaliação considera para os três fatores, gravidade, ocurrência e deteção, difere da escala tradicional da metodologia FMEA, escala esta que chega aos 10 valores. A escala de 5 valores presente nesta dissertação ocorre por motivos de hábituação prévia por parte dos colaboradores, sendo que, este tipo de avaliação feita ao longo dos anos no Grupo EDP sempre ocorreu numa escala de 5 valores e, por motivos internos, pretende-se que seja mantida.Tal ocorre por motivos de uniformização da perspetiva de quem preenche estes níveis no *software* ServiceNow, deste modo, a avaliação tem bases semelhantes apresentando assim o mesmo grau de comparação para todos os potenciais modos de falha. O sistema usa, ainda, estes valores numéricos para calcular quantitativamente respostas qualitativas de forma a apresentar informação intuitiva nos *dashboards* finais. É a aplicar estes dois valores, o financeiro e o percentual estatístico, que o *software* apresenta um valor financeiro verdadeiro, sendo este a expectativa de perda anual, que se correlaciona com as pontuações, situação esta explorada em seguida.

Para a avaliação da gravidade e ocorrência, os colaboradores preenchem diretamente no ServiceNow a sua perceção dos níveis correspondestes a esta avaliação tendo em conta o risco inerente que as potenciais falhas representam, esta avaliação é demonstrada no ponto seguinte, sendo este "5.3.2 - Implementação no *Software* ServiceNow". A pontuação adquirida pode ser observada na Tabela 5.2.

Tabela 5.4 - Classificação de ocorrência e critérios sugeridos

Nível de ocorrência	Valor estatístico máximo de percentagem	Classificação
Extremamente improvável	20%	1
Pouco provável	40%	2
Neutro	60%	3
Provável	80%	4
Extremamente provável	100%	5

Tabela 5.3 - Classificação da gravidade e critérios sugeridos

Nível de gravidade	Valor financeiro	Classificação
Muito baixo	$1,000,000.00	1
Baixo	$5,000,000.00	2
Moderado	$10,000,000.00	3
Alto	$20,000,000.00	4
Muito alto	$25,000,000.00	5

Relativamente à pontuação de deteção que os potenciais modos de falha em questão adquiriram, esta é feita relativamente aos controlos existentes cujo propósito é de deteção e não de prevenção de potenciais modos de falha. O Grupo EDP aposta, não só em controlos de deteção, como pode ser identificado na Tabela 5.2 e também nos anexos, sendo que, grande parte dos controlos subjacentes à norma em questão são controlos preventivos. Com isto a organização pretende evitar a concretização de ameaças reagindo às mesmas e responder à deteção de atividades anómalas.

Para a avaliação da deteção dos controlos detetivos considerados na tabela anterior, sendo estes "Sistema de deteção de credenciais inexistentes" e "Autenticação", seguiu-se os critérios estabelecidos na Tabela 5.5. Ambos os controlos apresentam uma componente detetiva visto que existe localização automática do lugar de ligação onde o indivíduo que se pretende conectar encontra, tanto dentro como fora da rede EDP. Ainda, caso a autenticação seja feita de fora dos limites da rede, é desencadeado, automaticamente, um processo programado com o objetivo de confirmar a identidade do colaborador, sendo este processo nomeado de "autenticação multifator", detetando assim quaisquer possíveis intrusos.

Tabela 5.5 - Classificação de deteção e critérios sugeridos

Nível de deteção	A probabilidade de os controlos detetarem a falha	Classificação
Quase certo	É quase certo que os controlos atuais detetarão o modo de falha	1
Alto	Alta probabilidade que os controlos atuais detetem o modo de falha	2
Moderado	Probabilidade moderada de que os controlos atuais detetarão a falha	3
Baixo	Baixa probabilidade que os controlos atuais detetem o modo de falha	4
Quase impossível	Nenhum controlo conhecido disponível para detetar o modo de falha	5

Tendo isto em consideração, classificou-se a deteção do potencial modo de falha "O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados" com a pontuação de 1 valor, ou seja, nível de deteção quase certo. Considera-se a classificação de 5 valores, nível de deteção quase impossível, qualquer potencial modo de falha cujos controlos são preventivos pois a componente de deteção de falhas é inexistente.

A Tabela 5.2, por fim, mostra ainda o cálculo do risco final, RPN, que resulta da multiplicação dos fatores mencionados até agora. A fórmula deste cálculo é demonstrada abaixo:

$$RPN = gravidade \times ocorrência \times deteção$$

5.3.2. Implementação no *Software* ServiceNow

Entidades

Antes de iniciar a programação de controlos, indicadores e riscos, é necessário definir, no *software*, quais os ativos a que estes são aplicados. Para o ponto de partida selecionado, é necessário não só nomear todas as aplicações em uso no Grupo EDP, como criar entidades relacionadas com as políticas e normas legislativas. Consequentemente, são criadas entidades de *governance* e de aplicações.

De forma a facilitar a associação entre riscos, controlos e entidades, o *software* ServiceNow, permite juntar entidades. Para tal, é criado um tipo de entidade (Entity Type). O tipo de entidade permite, assim, agrupar os ativos de informação em função das suas características ou propriedades, como por exemplo "área responsável" ou "contém dados pessoais", etc. As entidades (Entities) são, então, relacionadas automaticamente de acordo com as opções de filtragem configuradas pela equipa GRC. A Figura 5.4 possibilita a visualização do agrupamento das aplicações existentes na organização na área de Security & Risk.

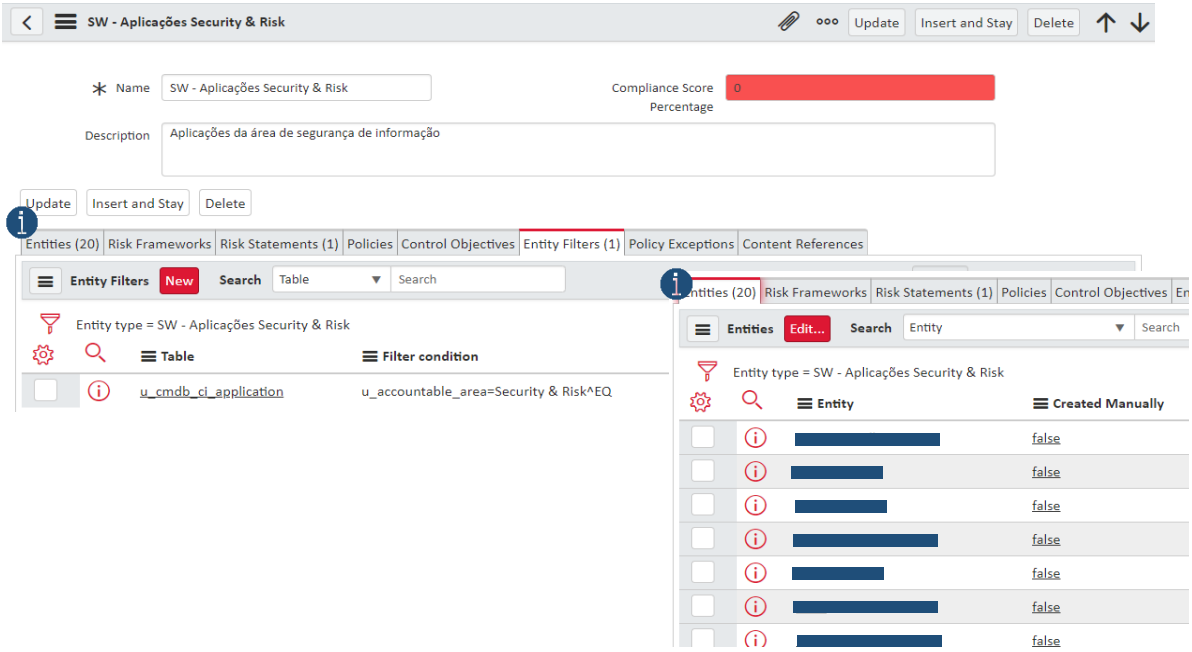


Figura 5.4 - Entities type e entities no ServiceNow

Riscos

No módulo do risco no ServiceNow é possível carregar os riscos associados aos efeitos dos potenciais modos de falha identificados. Após o carregamento massivo dos diversos riscos, que são implementados no so*ftware* em forma de declaração de risco (Risk Statement), é usada o tipo de entidade para combinar as declarações de risco e gerar, assim, todos os riscos referentes a cada entidade. Pode-se ainda relacionar as entidades a um *framework* de risco, que é uma agregação de declarações de risco com características comuns, como a relação mencionada entre o tipo de entidade e as entidades. Ao fazê-lo, o *software* associa automaticamente os riscos, as políticas e os objetivos dos controlos, referentes ao módulo *policy & compliance*, ao tipo de entidade selecionada para a associação.

O caso demonstrado em seguida é baseado em informação *standard* devido, mais uma vez, a motivos de confidencialidade e proteção de informação financeira da empresa. A Figura 5.5 representa uma declaração de risco referente ao risco de incêndio. Esta funcionalidade do ServiceNow permite ao colaborador sugerir, com a base numa perspetiva simples e subjetiva, a sua opinião sobre o nível de impacto ou gravidade e o nível de probabilidade ou ocorrência associados ao risco sob sua responsabilidade. A pontuação de risco é, assim, feita de um ponto de vista inerente e residual, segundo o pior caso de impacto e probabilidade, ou seja, o nível

de risco antes de qualquer medida de melhoria, *versus* o melhor caso de impacto e probabilidade, respetivamente.

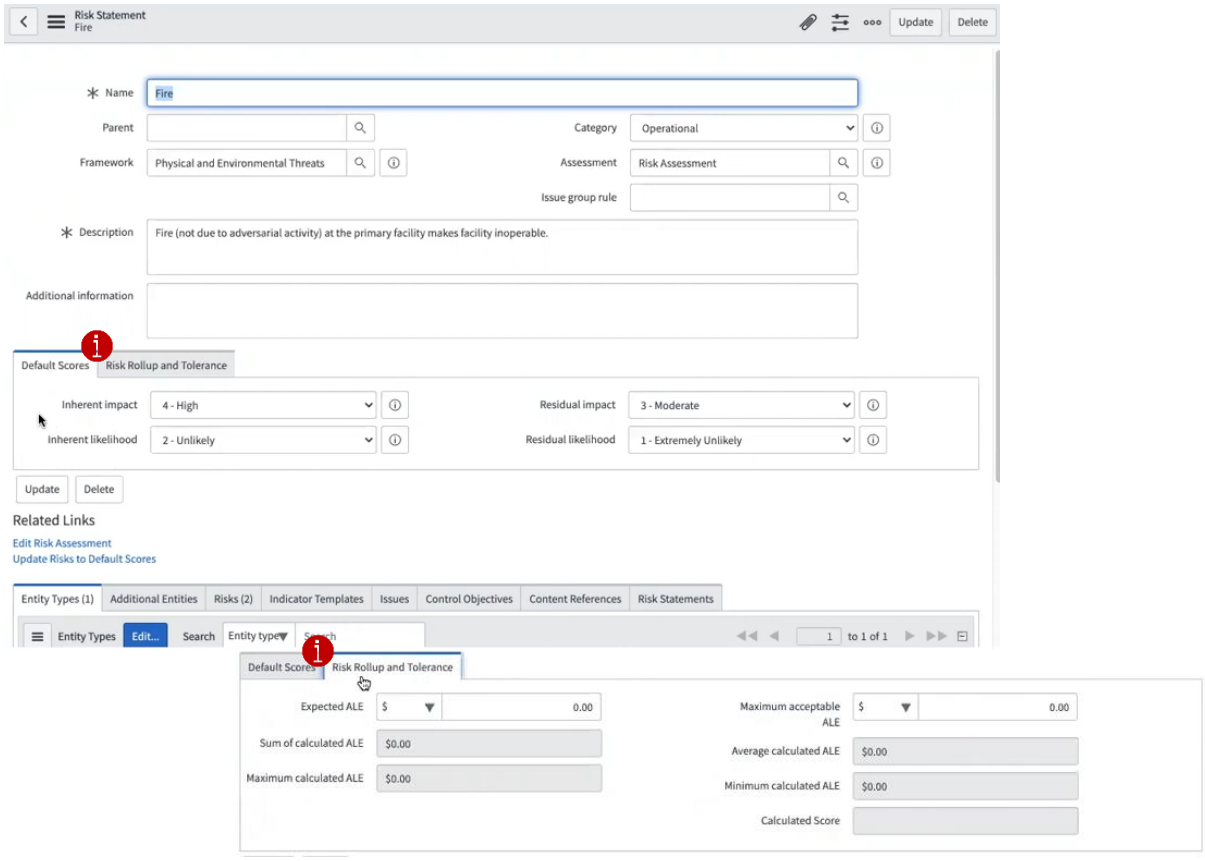


Figura 5.5 - Risk statement no ServiceNow

O "Risk Rollup and Tolerance" também presentes nesta secção do *software* e também representados na imagem, é onde é feita referência ao risco operacional do ponto de vista financeiro, ou seja, o que realmente é esperado a um nível agregado e o impacto financeiro desse risco operacionalmente.

Na Figura 5.6 é examinado o risco resultante da declaração de risco anterior após associação a uma entidade. O risco de incêndio, que é muito semelhante à declaração de risco de incêndio, herda muitas informações como a categoria e o próprio enunciado. A pontuação inicial é também herdada da declaração de risco sendo que todos os riscos provenientes dessa declaração têm uma perspetiva inicial compartilhada.

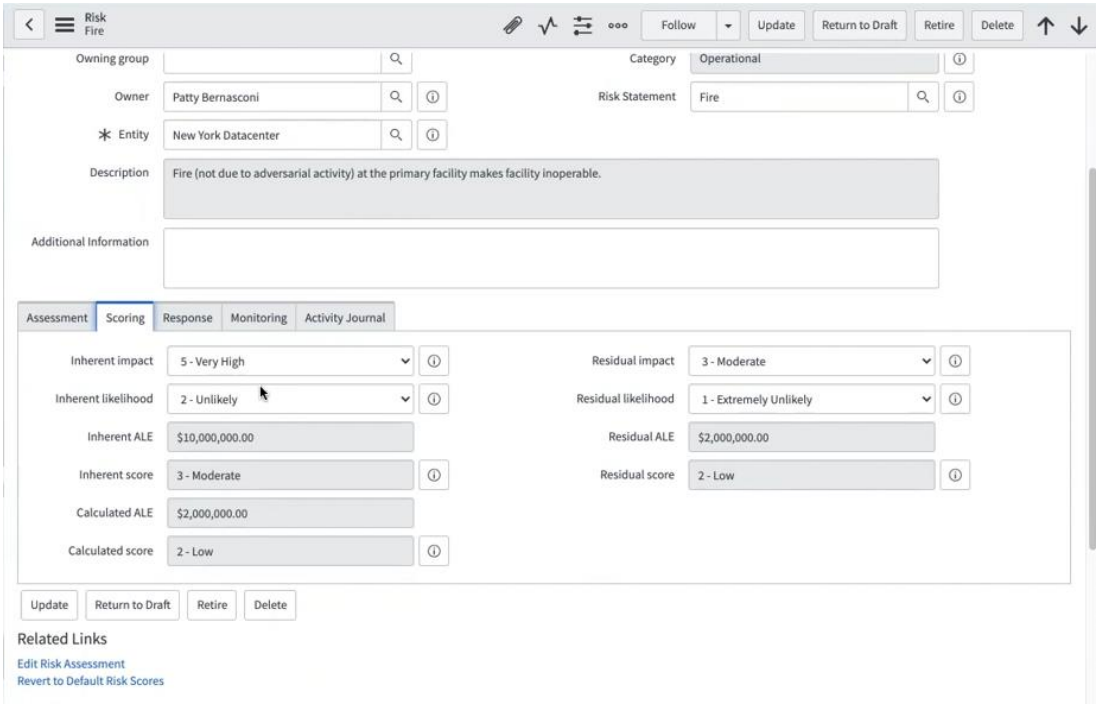


Figura 5.6 - Risco no ServiceNow

Nesta secção o colaborador pode reajustar o "Scoring" segundo a entidade específica em questão. É nesta fase que existe ajuste da pontuação residual, que visa o impacto do melhor cenário e a probabilidade baseada na perspetiva do responsável, e da pontuação inerente que, normalmente, é igual ao nível avaliado na declaração de risco "pai" e, provavelmente, não se altera, excetuando situações drásticas como o caso representado neste capítulo.

No exemplo, o impacto inerente de nível muito alto mas improvável, dá a pontuação inerente. Ao mesmo tempo, no lado residual, o nível de impacto moderado e probabilidade rara resulta na pontuação residual. Ambas as pontuações vão ajustar automaticamente a pontuação real do risco geral para a entidade, ou seja, permitem o cálculo automático ALE que representa o risco atual a que a organização está exposta. O risco atual calculado neste caso, onde todos os controlos se encontram em conformidade levando a uma percentagem de conformidade de 100%, é igual ao risco residual. Este é o objetivo principal de qualquer tipo de gestão do risco pois significa que o melhor caso possível está a ser mantido ao nível operacional diariamente e que os esforços de *compliance* mantém a empresa com o mínimo de risco possível. Esta situação, ter uma classificação de conformidade de 100% para todos os controlos relacionados a um risco, é, no entanto, muito rara.

Para efeitos desta dissertação são apenas utilizados os níveis da pontuação inerente e pontuação atual, para a avaliação de gravidade e ocorrência na fase "DO", como anteriormente mencionado, e avaliação de gravidade e ocorrência na fase "Resultados", respetivamente. Deste modo é possível verificar, através da comparação, do efeito das ações de melhoria e correção aplicadas.

A Figura 5.7 apresenta as diferentes opções a selecionar, pelo colaborador, de resposta ao risco.

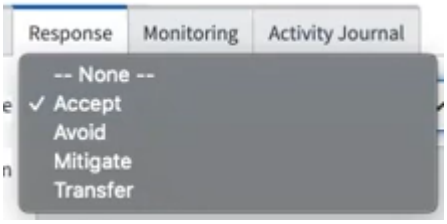


Figura 5.7 - Resposta ao risco no ServiceNow

Para todas as opções possíveis de seleção são criadas tarefas de resposta ao risco automaticamente no *software*. O risco pode, assim, ser aceite, aceitar é reconhecer que existe um risco e lidar com ele sem fazer nenhuma alteração. Para isso é criada uma tarefa de aceitação, esta assenta no plano ao qual se pretende socorrer caso ocorra o risco e como é suposto lidar e agir perante o mesmo. Esta requer a aprovação do proprietário do risco e da entidade. De seguida, a resposta ao risco passa por um processo de revisão e é criada uma exceção à política subjacente ao risco.

O risco pode também ser evitado. As tarefas de prevenção são pontos de documentação muito simples que defendem como evitar o risco, podem ser atualizações nos sistemas de versões mais recentes, aplicações de novos *patches*, etc. O próximo passo é, então, retirar o risco se o mesmo foi realmente evitado e deixar de existir, tal significa que um dos dois pontos, a vulnerabilidade ou a ameaça, desapareceu. Esta é provavelmente a resposta mais rara usada visto que evitar realmente um risco é uma tarefa com um nível de dificuldade elevado.

O colaborador pode ainda escolher mitigar o risco, nestas situações são criadas tarefas de mitigação. As tarefas de mitigação representam os planos a pôr em prática para a redução do risco, estes são assentes em ações de melhoria e ações de correção. Também este plano deve ser revisto e, após a revisão, são analisados os controlos necessários a implementar para atingir o objetivo delineado no plano de mitigação.

A última opção de resposta ao risco é transferir o risco, como por exemplo investir num seguro. Da mesma forma que nas opções anteriores de resposta, o *software* cria uma tarefa de transferência, nesta é possível fazer a escolha do vendedor de seguros, selecionar contratos, providenciar um plano de trabalho com o vendedor, etc. Após a finalização da tarefa de transferência e respetiva revisão, o risco pode ser simplesmente colocado em estado de monitorização. A monitorização é processada, ao contrário da monitorização dos controlos que apresenta uma data de validade, até que aconteça algo que torne necessária uma reavaliação. Os riscos são, assim, deixados neste estado até que sejam *retired*.

Controlos

De seguida é feita a implementação no *software* dos controlos identificados como essenciais à prevenção ou deteção dos potenciais modos de falha.

Em seguimento ao exemplo anteriormente indicado, para os 2 potenciais modos de falha selecionados, são definidos 4 controlos. As imagens abaixo demonstram a configuração do controlo "Autenticação" no ServiceNow.

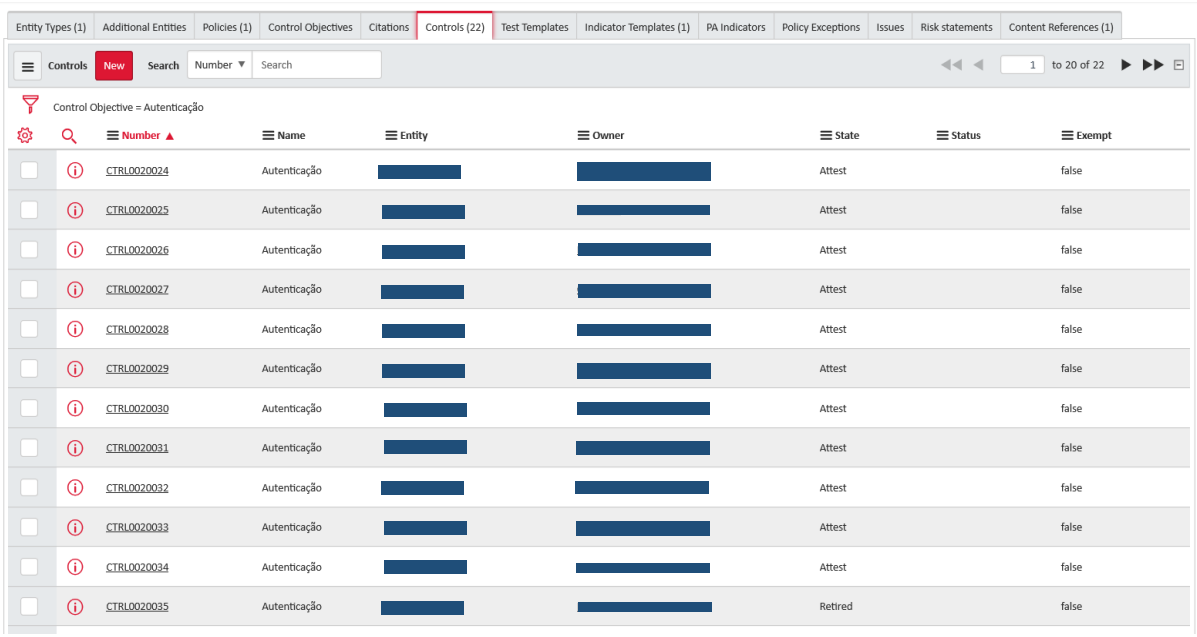


Figura 5.8 - Configuração do objetivo do controlo "Autenticação" no ServiceNow

A Figura 5.8 apresenta o objetivo do controlo. Neste campo é possível descrever o controlo em si em associação com a regra ou princípio do qual este foi originado. O *software* permite ainda, não só categorizar e classificar o objetivo do controlo, como também verificar o estado da conformidade do mesmo, em termos de percentagem de *compliance*, este parâmetro é utilizado na fase "CHECK" do plano PDCA. Ainda na Figura 5.8 é possível observar duas secções do objetivo do controlo referentes à associação entre este e o tipo de entidade ao qual é aplicável e a política ou norma da qual este descende.

O objetivo do controlo, ao ser associado ao tipo de entidade configurado para todas as aplicações, multiplica-se automaticamente em controlos individuais, consoante o número de entidades a que o objetivo do controlo foi associado, neste caso, o número de aplicações.

A Figura 5.9, ainda pertencente ao campo do objetivo do controlo "Autenticação", apresenta a secção dos controlos individuais automaticamente criados pelo ServiceNow devido à associação entre o objetivo do controlo e o tipo de entidade impulsionada anteriormente. Deste modo são estabelecidos 22 controlos, cada um igual ao objetivo do controlo mas referente a uma aplicação específica dentro do Grupo EDP.

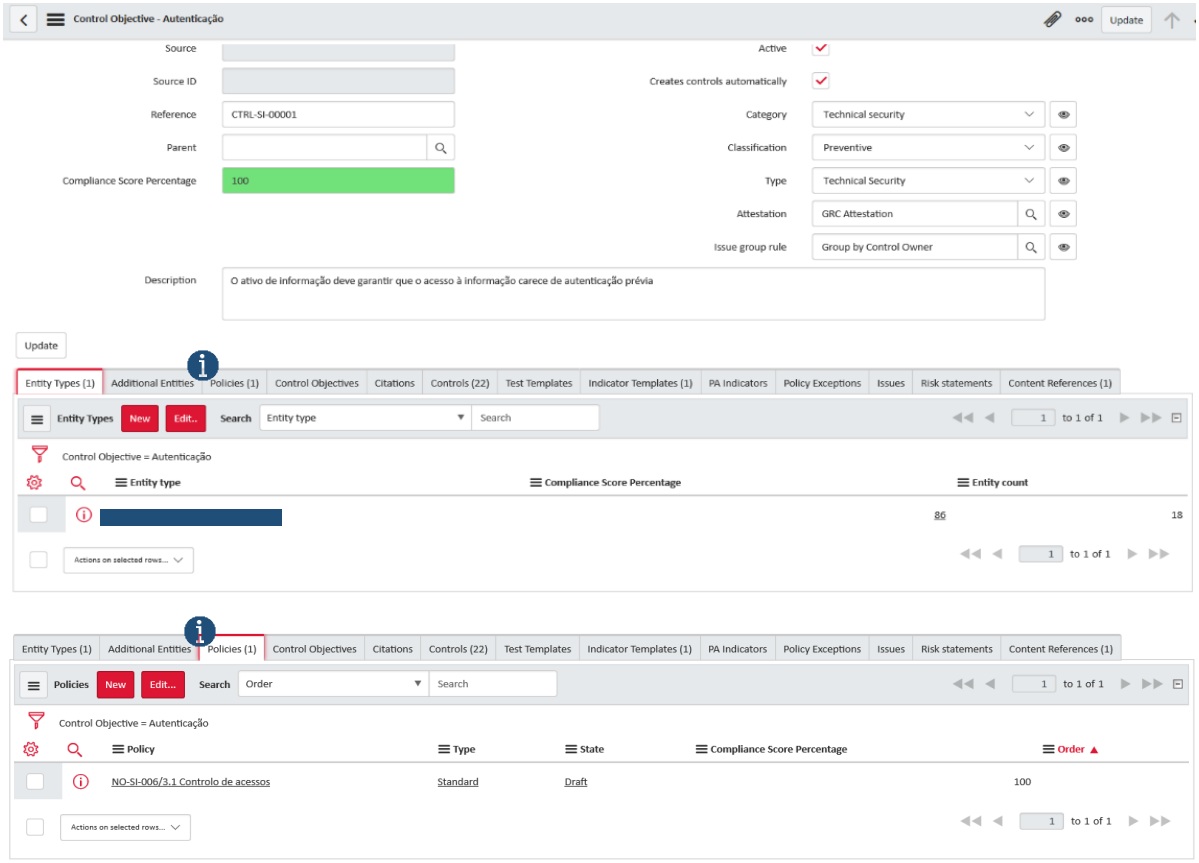


Figura 5.9 - Multiplicação automática dos controlos "Autenticação" no ServiceNow

O objetivo do controlo expõe ainda o *template* do indicador associado, que, para o objetivo do controlo em questão, é nomeado como "Autenticação prévia" como demonstrado na Figura 5.10. O *template* do indicador segue o mesmo processo de multiplicação ocorrente na conceção de controlos, ou seja, existe a criação de indicadores como consequência da ligação às diversas entidades. Este processo é abordado em detalhe na fase "CHECK" do plano PDCA visto que serve motivos de monitorização através de pedidos de evidência aos colaboradores responsáveis pelas entidades interligadas.

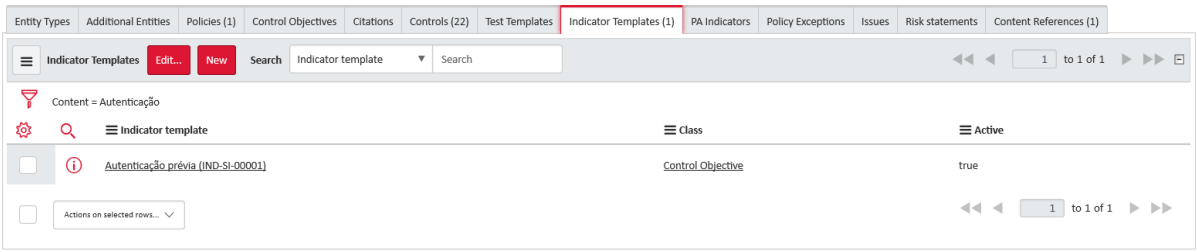


Figura 5.10 - Indicador "Autenticação prévia" no ServiceNow

Acrescenta-se ainda o facto de que o *software* permite adicionar *tags* virtuais a qualquer tipo de registo definido em qualquer módulo do ServiceNow. Na Figura 5.11 existe referência à ISO/IEC 27001:2013 visto ser esta a base de todos os normativos de *governance*, *risk* e *compliance* da organização.

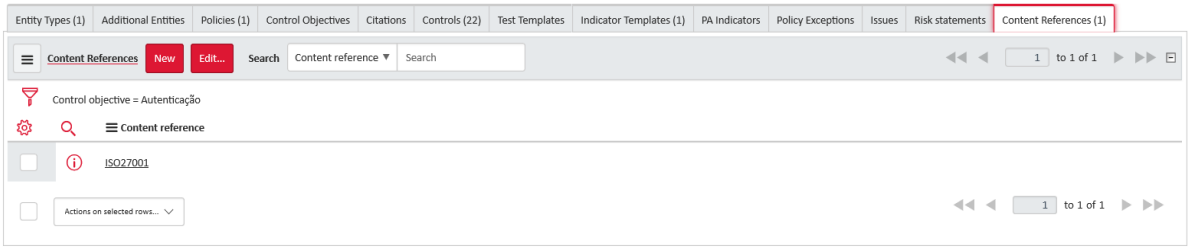


Figura 5.11 - Content references do objetivo de controlo "Autenticação" no ServiceNow

Esta marcação na secção de "Content Reference" permite filtrar as marcações de conteúdo referido de forma a identificar os registos usados em cada aplicação. Com esta funcionalidade é ainda possível elaborar relatórios automaticamente de integrações específicas dos registos relevantes a estes. Consequentemente, ao marcar todos os objetivos do controlo e outros registos, como os riscos, o processo de atualização da conformidade da empresa perante novas alterações regulamentares é simplificado visto que os dados referentes a qualquer normativo nacional ou internacional podem ser agregados e trabalhados através da aplicação de um filtro.

5.4. CHECK

Na fase "CHECK" do plano PDCA é feita a monitorização automática e manual dos controlos previamente estruturados na fase "DO". Acrescenta-se também a esta fase o preenchimento da coluna "Efetividade dos Controlos", esta célula da metodologia FMEA é diretamente relacionada com o estado do controlo sugerido automaticamente pelo *software* ServiceNow.

5.4.1. Implementação da Metodologia FMEA

Como apresentado no ponto anterior, e segundo o exemplo a ser seguido neste capítulo, o controlo "Autenticação" apresenta uma percentagem de *compliance* de 100%, como mencionado anteriormente, esta é visível na Tabela 5.6. Tal pontuação implica que, no teste deste mesmo controlo, que neste caso é feito através de um *template* de indicador manual, todas as aplicações "passaram" o teste, ou seja, todas as aplicações estão configuradas para pedir autenticação ao utilizador, estando, por isso, *compliante* com a legislação.

Tabela 5.6 - FMEA exemplo fase "CHECK"

PLAN		DO									CHECK
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos
Função	Potenciais Modos de Falha					Prev.	Det.				
Controlar Acessos	O acesso à informação, aos sistemas e recursos de TI do Grupo EDP, e aos seus processos de Negócio não é controlado com base nos requisitos de Segurança da Informação e de Negócio, bem como nos requisitos de legislação e regulamentação	Acesso ilegítimo	1	Existência de controlos de acesso ineficientes devido a incoerências com a legislação	2	Procedimentar a articulação com a área de Segurança de Informação do Grupo EDP	-	5	10	*Governance*	60%
						Procedimentar o controlo de acesso à informação					100%
	O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados	Acesso ilegítimo	3	Acesso ilegítimo por incorreta restrição de utilizadores	1	-	Sistema de deteção de credenciais inexistentes	1	3	Aplicações	100%
							Autenticação				100%

A restante avaliação de efetividade dos controlos, tanto dos apresentados na metodologia FMEA neste capítulo como dos correspondentes ao resto da aplicação do normativo referente ao Controlo de Acessos expostos nos Anexos, seguem o mesmo processo orientador. Pelo que, os valores apresentados na coluna "CHECK" da ferramenta são fundamentados pela obtenção de evidências, por parte dos colaboradores de Grupo EDP, da aplicação dos controlos. O *software* compila a informação e dados recebidos e aceites através das evidências submetidas com o objetivo de determinar a percentagem de *compliance* de determinado objetivo do controlo tendo em conta o número de controlos efetivos.

A avaliação da efetividade dos controlos, transcritos em massa para o *software* ServiceNow, é, assim, calculada de forma automática através de pedidos de evidências manuais. Acontece ainda a possibilidade de criação de *templates* de indicadores automáticos, onde, em vez do pedido de evidências manual, o próprio *software* recolhe informação e verifica os controlos segundo fórmulas e programações definidas. A existência de *templates* de indicadores automáticos é, no entanto, mais comum na Norma de Gestão de Ativos, visto que as entidades já estão programadas e caracterizadas no ServiceNow, permitindo assim a pesquisa automática.

5.4.2. Implementação no *Software* ServiceNow

Indicadores

A monitorização, como anteriormente referido, é feita maioritariamente através de indicadores manuais. Os responsáveis pelos ativos necessitam, então, de confirmar e evidenciar periodicamente que o controlo está implementado. Este processo é feito por cada entidade, ou seja, por cada ativo de informação.

A Figura 5.12 apresenta a configuração do *template* do indicador "Autenticação prévia" assim como o processo de multiplicação do mesmo nos vários indicadores representativos das várias entidades, neste caso aplicações. Na configuração do *template* do indicador, a equipa GRC, mais precisamente os elementos internos do Grupo EDP, inseriu as instruções necessárias à resposta, por parte dos colaboradores, da tarefa do indicador. Inseriu-se ainda a data de envio dos indicadores resultantes do *template* do indicador aos responsáveis. A calendarização da solicitação de provas de implementação dos controlos é feita mensalmente por norma ou política, esta tem ainda uma validade de 15 dias, pelo que, após o término deste período e em caso de falta de resposta, o controlo é dado como não *compliant*. Cada solicitação é ainda enviada anualmente de forma a cumprir com a legislação e a garantir conformidade nas auditorias, estas também anuais.

Ao responsável por cada aplicação é, então, enviada uma tarefa do indicador previamente calendarizada pela equipa GRC. A Figura 5.13 demonstra o indicador "Autenticação prévia" referente a uma aplicação. Esta configuração é feita automaticamente pois é descendente do *template* do indicador "Autenticação prévia" anteriormente estabelecido.

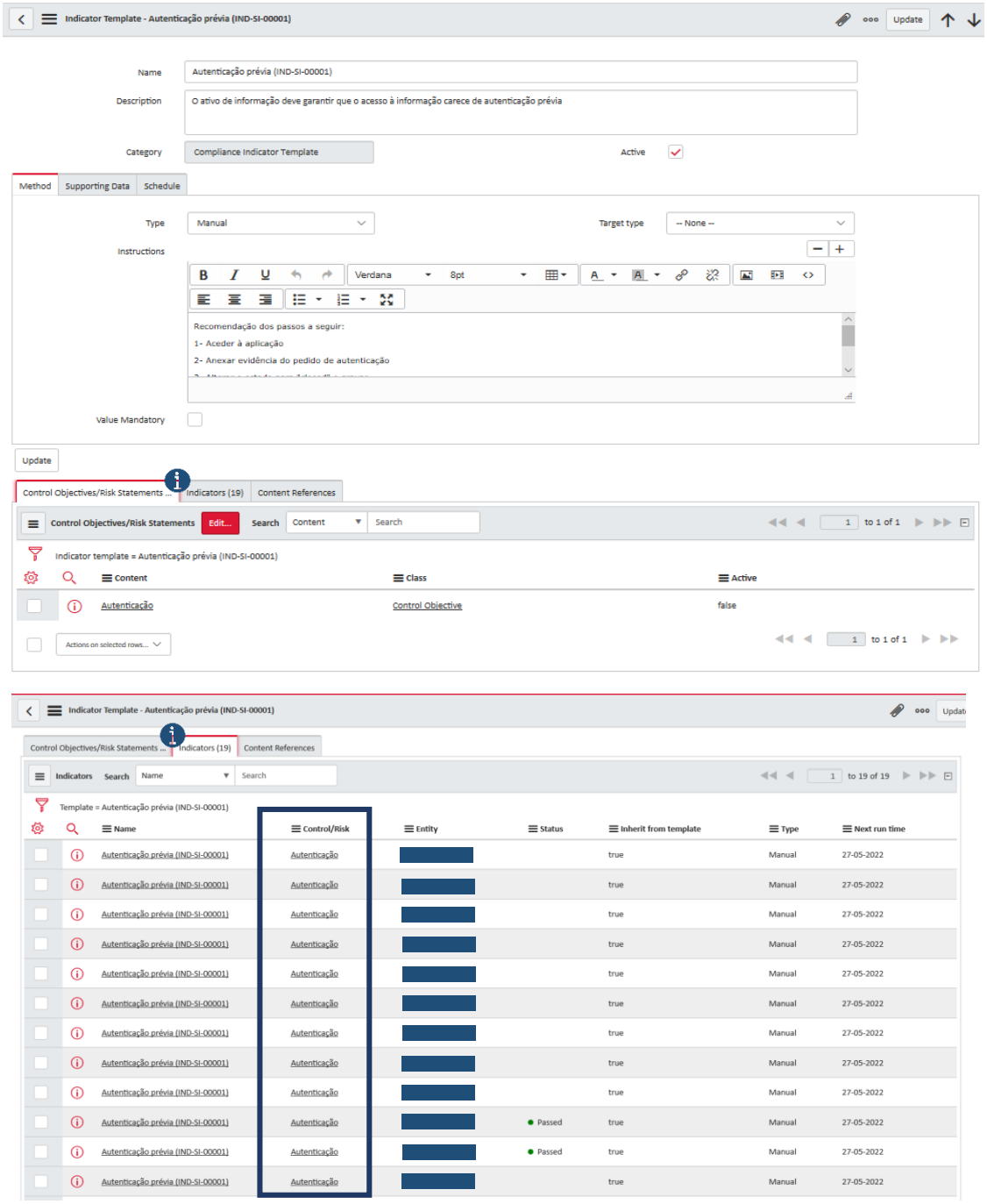


Figura 5.12 - Configuração do template do indicador "Autenticação prévia" no ServiceNow

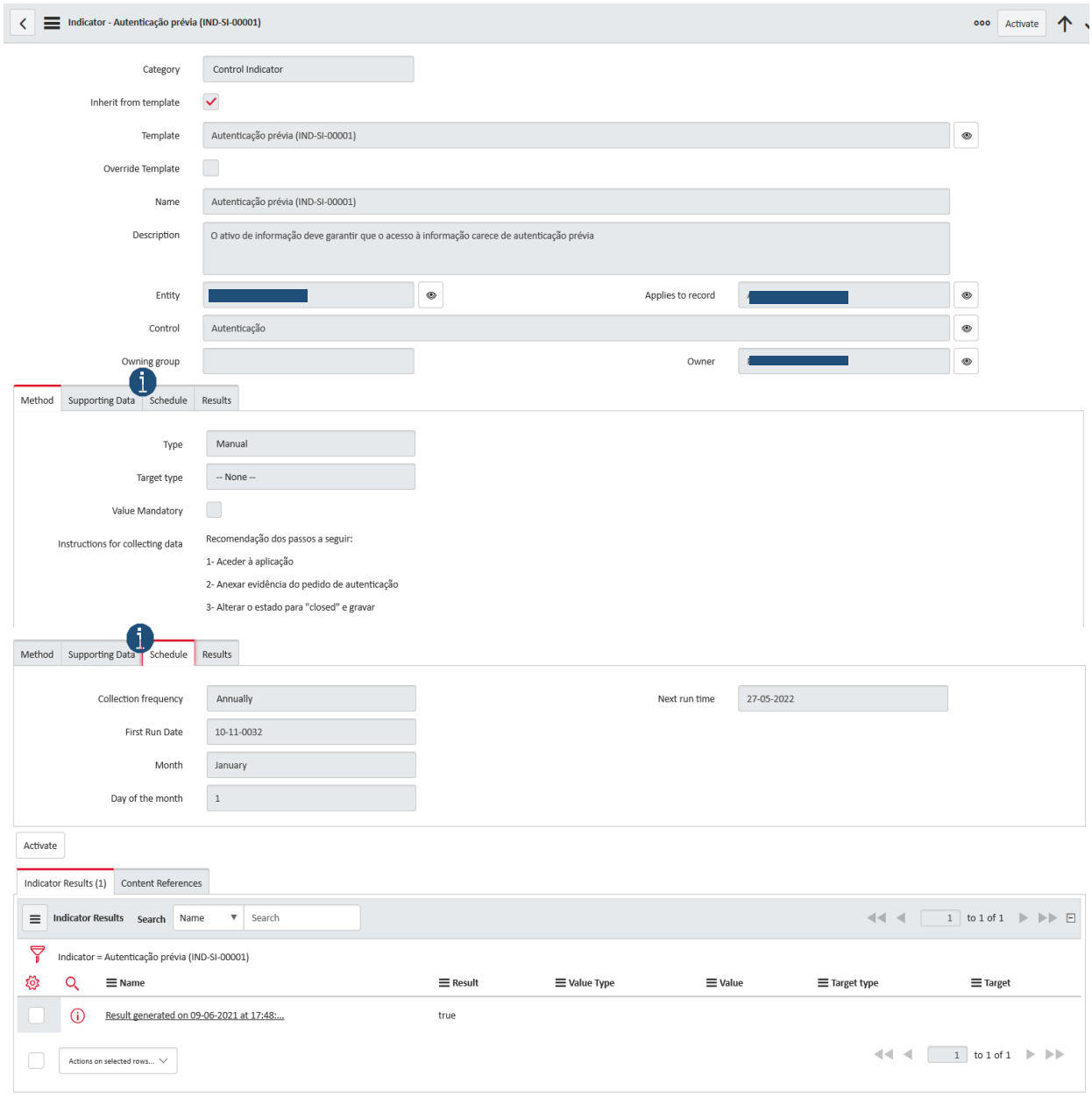


Figura 5.13 - Indicador "Autenticação prévia" referente a uma aplicação no ServiceNow

O responsável procede assim à resposta da tarefa do indicador onde indica o estado da sua implementação relativamente à aplicação pela qual se encontra encarregue e anexa evidências dessa mesma indicação, caso este esteja implementado como o caso demonstrado na Figura 5.14.

Nos casos em que o controlo não se encontra efetivo, processo detalhado na fase "ACT" no plano PDCA, duas opções podem ser seguidas. Pode ser criada uma exceção à regra, por motivos de não aplicabilidade de um controlo a uma certa entidade, que posteriormente deve ser aceite, ou é criado um problema (Issue), nestes casos ações de melhoria ou correção devem ser tidas em consideração.

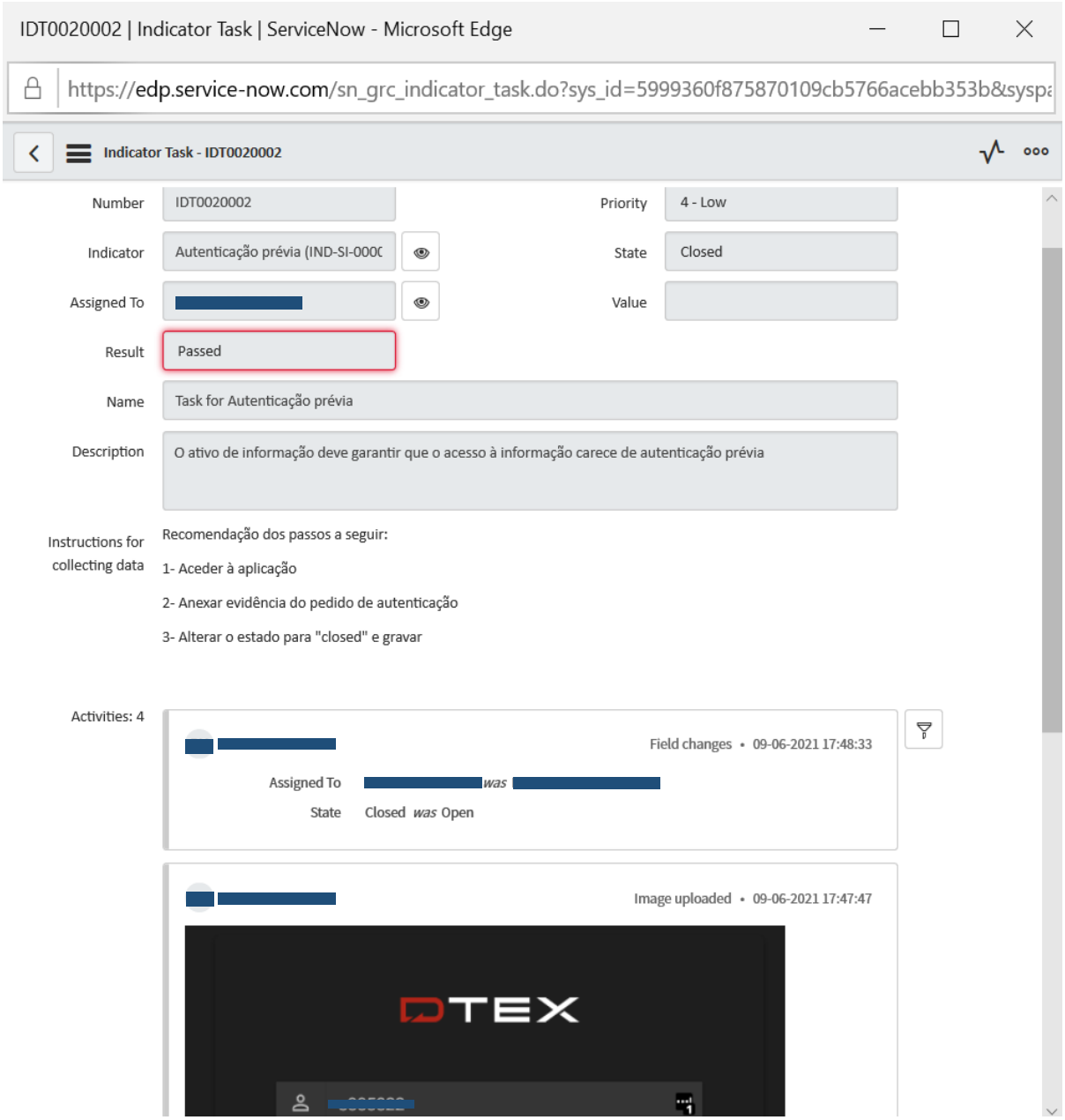


Figura 5.14 - Resposta ao indicador "Autenticação prévia" referente a uma aplicação no ServiceNow

Controlos *Attestations*

Como mencionado no Capítulo 3, mais precisamente na Secção 3.3.6.3 – Módulo de *Policy & Compliance* do ServiceNow, o *software* ServiceNow permite que a avaliação da efetividade dos controlos seja feita recorrendo não só a indicadores manuais e automáticos como também a *attestations*.

A equipa GRC decidiu aproveitar a diversidade de opções de evidências de controlos implementados para diferenciar o tipo de evidências pedidas aos colaboradores responsáveis por entidades ou ativos. Desde modo uniformizou-se o envio de indicadores manuais com o propósito de obter provas visuais e individuais, ou seja, por entidade, da implementação dos

controlos, como demonstrado anteriormente. Relativamente ao envio de *attestations*, este é feito com o objetivo de obter a documentação processual de como os controlos devem ser implementados nas operações.

Visto que a abordagem GRC presentemente estudada nesta dissertação serve ainda os propósitos iniciais de todo o projeto e a escalabilidade deste serviço a toda a empresa EDP, incluindo EDP *geographies*, será incluída posteriormente, a aplicação de *attestations* não é, ainda, justificável. Tal ocorre devido ao facto de que toda a documentação processual existente na unidade DGU, unidade de implementação inicial da abordagem GRC no Grupo EDP, já é conhecida pelos elementos da área de Security & Risk, sendo que, o pedido de demonstração da mesma contraria a lógica de custo-benefício desta mesma atividade.

A funcionalidade *attestaions* é, portanto, útil após a expansão a outras áreas e unidades do Grupo EDP. Isto é devido à possibilidade de existência de outros procedimentos diferentes de materialização dos controlos existentes em normas e políticas de alto nível. Desta forma, ao pedir resposta à efetividade de um controlo numa outra área ou geografia do Grupo que é procedimentado de forma diferente, são enviados uma *attestation* e um indicador manual. A resposta a este controlo pelo colaborador deve envolver o anexo do documento que descreve o procedimento utilizado pela área da EDP em questão, como resposta à *attestation*, e evidências da implementação desse mesmo procedimento aos ativos que este abrange, como resposta ao indicador manual.

5.5. ACT

Cada ciclo do plano PDCA só é fechado quando todos os problemas possíveis são corrigidos ou todas as melhorias consideradas necessárias são implementadas, ou seja, após a finalização da fase "ACT".

Nesta última fase de cada ciclo é feita a análise do estado dos controlos e riscos associados. Pretende-se, assim, identificar as ações necessárias para atingir o maior nível de conformidade geral possível e aceitável para o Grupo EDP.

Este é um processo recorrente e circular ao longo do tempo, sendo que, a melhoria contínua é sempre um objetivo desejável a alcançar na organização. Deste modo, é nesta fase que são encontrados e estudados os problemas consequentes da falta de efetividade dos controlos. Pretende-se resolver os problemas através de medidas corretivas ou de melhoria, estas podem passar por modificar controlos existentes, reavaliar o risco, implementar novos controlos, etc. Em seguida é demonstrado como o *software* ServiceNow expõe os problemas (Issues) encontrados automaticamente e o processo de tratamento dos mesmos. No entanto, primeiramente é preenchida a metodologia FMEA na fase "ACT" seguindo as informações obtidas e calculadas pelo *software* para a efetividade dos controlos.

5.5.1. Implementação da Metodologia FMEA

Como é possível analisar na Tabela 5.7, apenas um dos controlos mencionados não apresenta a totalidade de *compliance* em termos de avaliação de efetividade. "Procedimentar a ar-

ticulação com a área de Segurança de Informação do Grupo EDP" apresenta, segundo o ServiceNow, 60% de *compliance*, devido a tal, foram identificadas estratégias e deduzidas ações concretas para aumentar a percentagem atual de efetividade. Estas últimas podem ser verificadas também na Tabela 5.7, nas colunas correspondentes à fase "ACT".

Tabela 5.7 - FMEA exemplo fase "ACT"

PLAN		DO									CHECK	ACT	
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos	Ações de Melhoria	Ações de Correção
Função	Potenciais Modos de Falha					Prev.	Det.						
Controlar Acessos	O acesso à informação, aos sistemas e recursos de TI do Grupo EDP, e aos seus processos de Negócio não é controlado com base nos requisitos de Segurança da Informação e de Negócio, bem como nos requisitos de legislação e regulamentação	Acesso ilegítimo	**1**	Existência de controlos de acesso ineficientes devido a incoerências com a legislação	**2**	Procedimentar a articulação com a área de Segurança de Informação do Grupo EDP	-	**5**	**10**	*Governance*	60%	Motivar a resposta aos indicadores	Aumentar a regularidade das reuniões de equipa
						Procedimentar o controlo de acesso à informação					100%	-	-
	O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados	Acesso ilegítimo	**3**	Acesso ilegítimo por incorreta restrição de utilizadores	**1**	-	Sistema de deteção de credenciais inexistentes	**1**	**3**	Aplicações	100%	-	-
							Autenticação				100%	-	-

Analisou-se que a percentagem de efetividade correspondente ao controlo em questão não é apenas consequente do processo necessário ao controlo em si mas também devido à

falta de resposta atempada, por parte dos colaboradores do Grupo EDP, ao indicador manual enviado. Quando a resposta ao pedido de evidência de implementação do controlo passa a validade da data indicada no indicador manual, definida pela equipa GRC como 15 dias úteis, o indicador é fechado e registado como "failed", ou seja, reverte-se no controlo como não *compliante*, que por sua vez, diminui a percentagem de efetividade do objetivo do controlo.

Para colmatar esta ocorrência, a equipa GRC definiu estratégias de comunicação com a unidade DGU com o objetivo de motivar a resposta atempada aos indicadores que lhes são atribuídos. A ação de melhoria incluí, portanto, o envolvimento dos membros pertencentes a esta unidade do Grupo nos benefícios da abordagem GRC, não só para a organização como também para os seus próprios trabalhos e atividades diárias.

Em seguida e de forma a evoluir a articulação com a área de segurança de informação do Grupo EDP, estabeleceu-se uma medida corretiva assente no aumento da comunicação entre os membros da equipa. Assim, ao aumentar a regularidade das reuniões de equipa, é possível manter uma atualização mais constante das atividades de cada colaborador, interações e alinhamentos necessários.

5.5.2. Implementação no *Software* ServiceNow

Issue

Um issue surge automaticamente no *software* sempre que um controlo ou indicador não se encontra *compliant* ou falha, respetivamente. Tais situações podem ocorrer por diversos motivos como a falta de resposta atempada às *attestations* enviadas ou aos indicadores manuais, a falta de efetivada dos objetivos dos controlos, a falta de coerência considerando os riscos associados, entre outros como demonstrada na Figura 5.15.

Sempre que ocorre a criação automática de um issue, o colaborador responsável pela causa do mesmo deve analisá-lo e dar resposta de modo a que este possa ser revisto e fechado. O objetivo permanece na existência reduzida de issues no ServiceNow que, nem sempre, é uma situação controlável tendo em conta os diversos fatores associados a esta.

Como é ainda demonstrado na Figura 5.15, é possível determinar a prioridade do issue em questão, neste caso em seguimento na presente dissertação, a falha de um indicador da aplicação UBA encontra-se com pouca prioridade.

A resposta a este e aos outros issues reverte-se em duas opções que o colaborador responsável deve selecionar. A primeira centraliza-se na remediação do problema, neste sentido é criada uma *remediation task* com os passos a seguir para o caminho de resolução pretendido. A segunda opção é baseada na aceitação consciente do problema em destaque, sendo que, é criado uma *policy exception* que deve ser aceite pela gestão e cujo propósito é documentar a exceção encontrada e justificar a mesma. É abaixo demonstrada a opção selecionada para este caso.

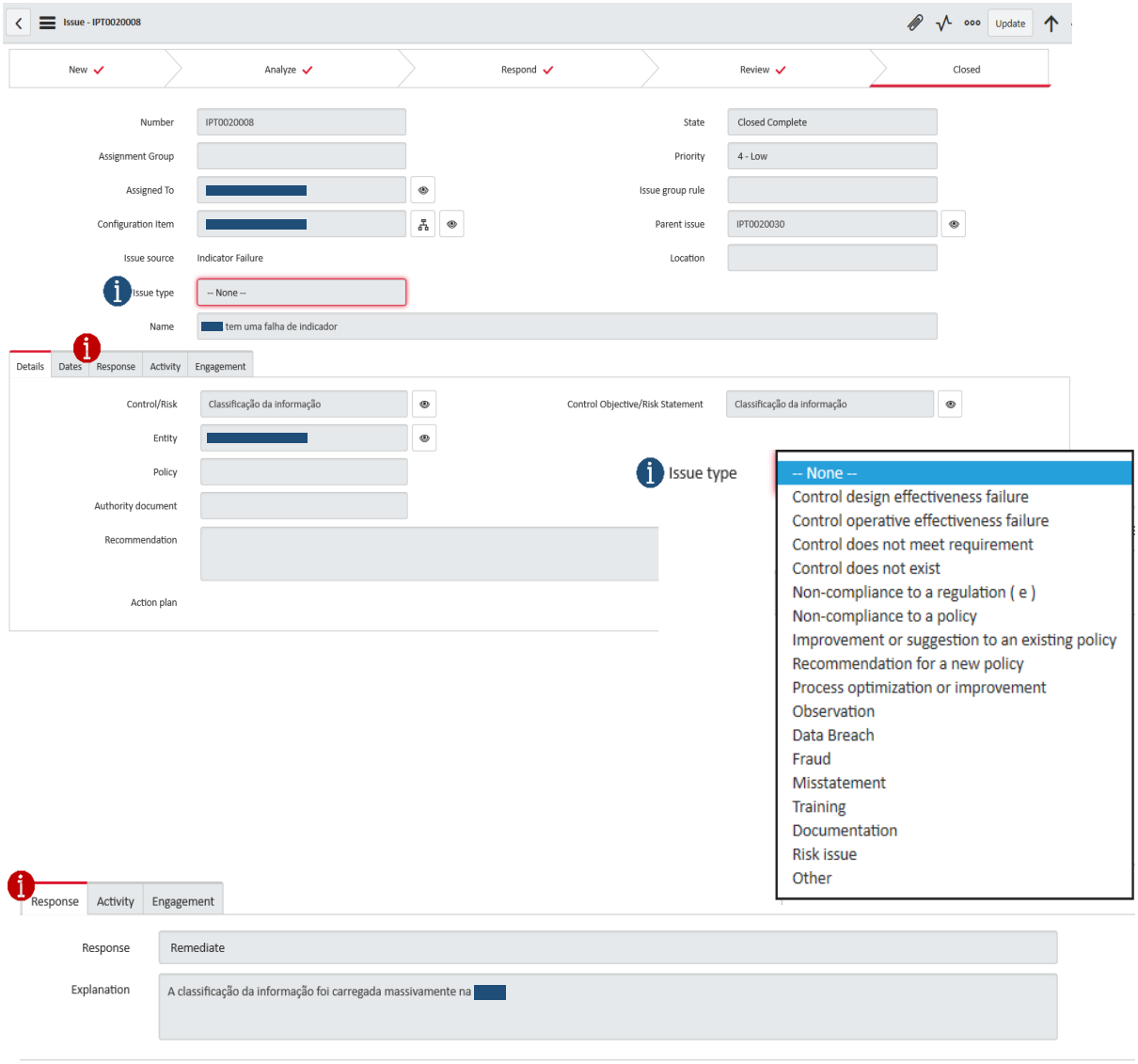


Figura 5.15 - Issue fechado no ServiceNow

5.6. Resultados

Como resultado da implementação da abordagem GRC acompanhada pela aplicação da metodologia FMEA segundo a lógica do ciclo PDCA desenvolvido, obteve-se uma melhoria significativa entre os resultados do cálculo do RPN na secção "DO" e os resultados do mesmo cálculo após a implementação de ações de melhoria ou correção, para a secção "Resultados", como pode ser comprovado em anexo e facilmente analisado por observação do gráfico representado na Figura 5.16, para a Norma Controlo de Acessos. O Figura 5.16 demonstra, assim, a compação entre os valores de RPN cálculados nas duas secções da FMEA, que, como se pode confirmar, espelham o sucesso da presente implementação na maioria dos potênciais modos de falha identificados. É importante ainda referir que em muitos dos casos em que o valor do cálculo do RPN se mantém idêntico é devido a critérios de aceitação do risco, decididos por colaboradores experientes.

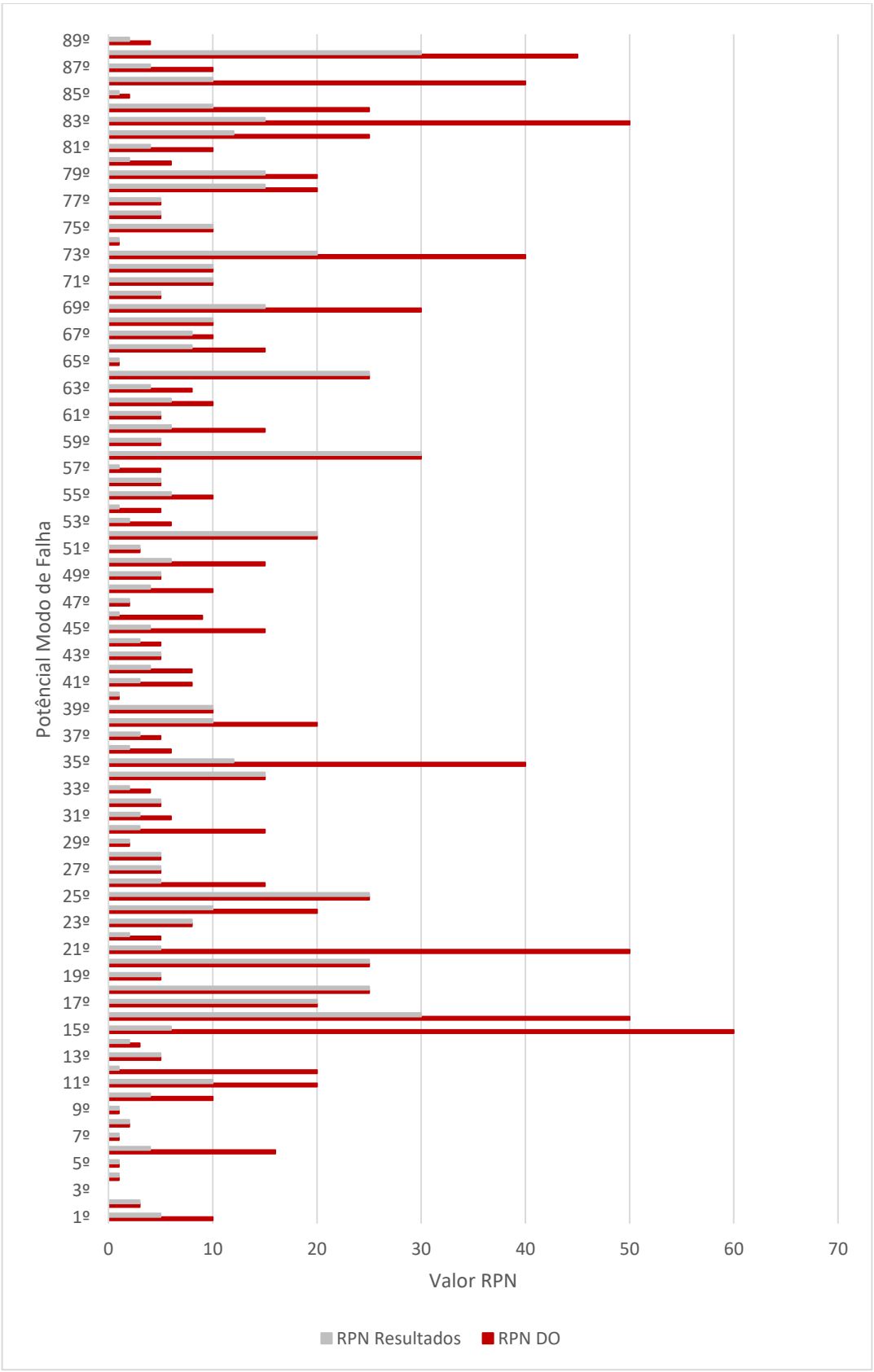


Figura 5.16 - Comparação dos valores cálculados de RPN

Em seguida é apresentada a visão holística mencionada em formato de *dashboard* para os diferentes dados com que o *software* opera.

Iniciando pelo *dashboard* de risco, este mostra os resultados das avaliações de risco e do processamento de risco num ambiente normal. Os painéis são muito complexos, pelo que é possível analisar o risco de várias perspetivas, na Figura 5.17 a análise é feita do ponto de vista qualitativo. São analisados, não só os cinco níveis de impacto ou gravidade, de muito baixo a muito alto, assim como os cinco níveis de probabilidade ou ocorrência, de extremamente improvável a extremamente provável, sendo que o *software* apresenta o cálculo da prioridade baseada nesses dois conceitos. É importante referir que a informação exposta neste capítulo é informação *standard*, pelo que não representa a realidade do Grupo EDP devido à privacidade justificável da mesma.

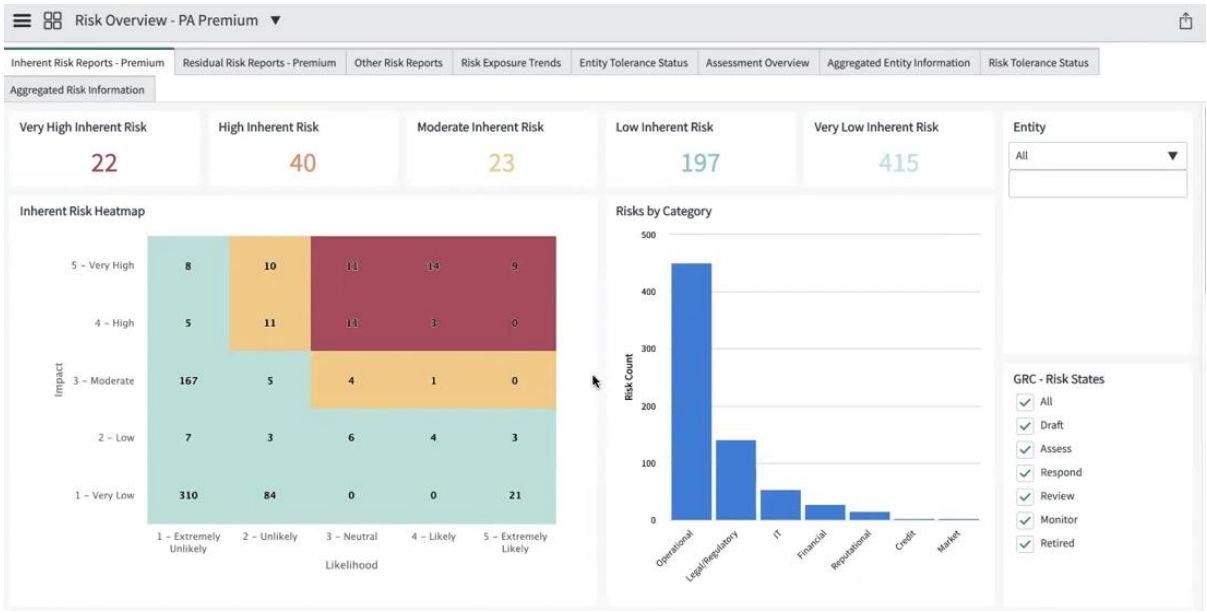


Figura 5.17 - Dashboard de risco inerente no ServiceNow

Relativamente à informação referente na Figura 5.17, do ponto de vista de um gestor de risco, é preferível abordar os 9 riscos muito altos e extremamente prováveis antes de abordar os 310 riscos não tão relevantes. Esta exposição de informação auxilia a tomada deste tipo de decisões, decisões de priorização de medidas de melhoria ou correção a serem tomadas.

Existem, ainda, relatórios fornecidos pelo ServiceNow que dependem somente de dados quantitativos, o caso do gráfico representado na Figura 5.18. Este gráfico de bolhas analisa a expectativa de perda única que está nos bastidores quanto ao impacto e a taxa anual de ocorrência, sendo esta a percentagem da probabilidade.

Figura 5.18 - Gráfico de bolhas no ServiceNow

Os gráficos informativos representados assentam, então, em riscos internos de um ponto de vista inerente, ou seja, representam a análise do pior cenário onde é definido o pior nível de impacto possível e o pior nível de probabilidade possível. Por outro lado, a Figura 5.19 representa o alvo onde a empresa deseja encontrar-se, o risco residual. Pretende-se que o risco residual seja muito inferior ao risco inerente pois, o primeiro, está assente numa situação de exposição ideal onde todos os controlos estão em conformidade, a mitigação do risco é feita tanto quanto possível assim como a transferência do risco é feita tanto quanto a responsabilidade sobre o mesmo o permite e as medidas necessárias para evitar todas as vulnerabilidades estão a ser tomadas e realizadas corretamente. O risco residual representa, assim, o melhor cenário possível.

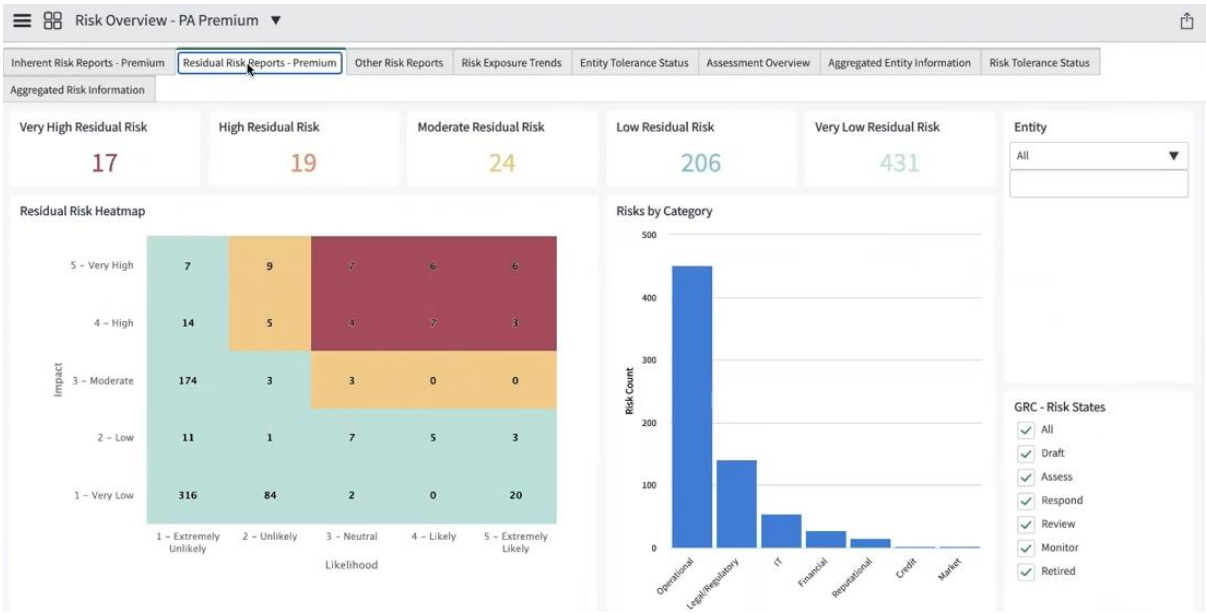


Figura 5.19 - Dashboard de risco residual no ServiceNow

A diferença entre o risco inerente e o risco residual, sem o módulo *policy & compliance*, é, basicamente, a ideia de que foi feito tudo o que era possível.

Relativamente ao módulo de *policy & compliance*, o *software* permite obter uma *overview* através de *dashboard* de *compliance* para a organização. Esta análise pode ser feita através de uma série de fontes regulatórias diferentes, como mostra o gráfico "Compliance by Authority Document" incluído na Figura 5.20. É, portanto, analisada a conformidade geral dos controlos aplicados na empresa. Mais uma vez são apresentados dados e gráficos padrão e, por isso, não representativos da informação referente ao Grupo EDP.

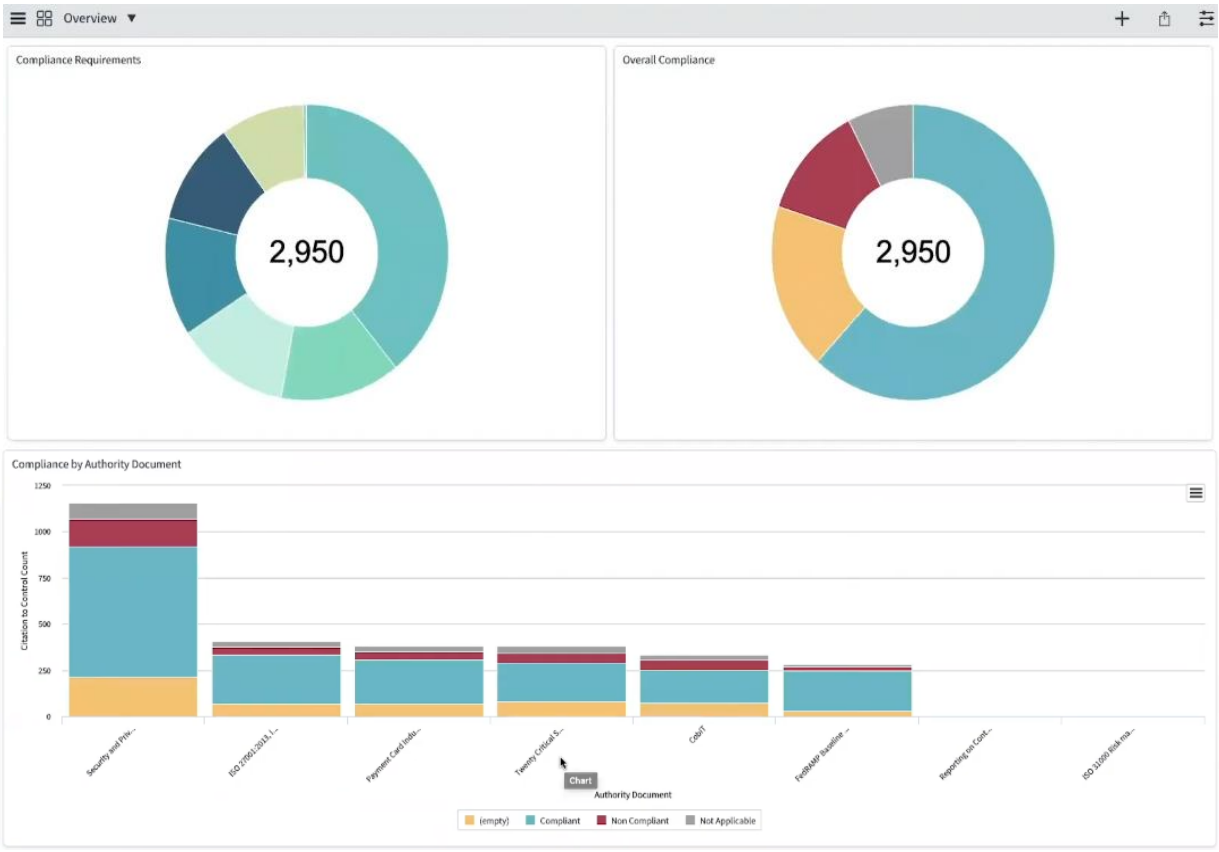


Figura 5.20 - Dashboard de compliance no ServiceNow

Do ponto de vista de *policy*, o *software* cria *dashboards* semelhantes e com o mesmo tipo de dados, mas, neste campo, do ponto de vista das políticas internas. É possível observar, na *overview* da secção das políticas, representada na Figura 5.21, uma visão geral dos controlos isentos ou exceções de políticas, as percentagens de pontuação de conformidade, etc.

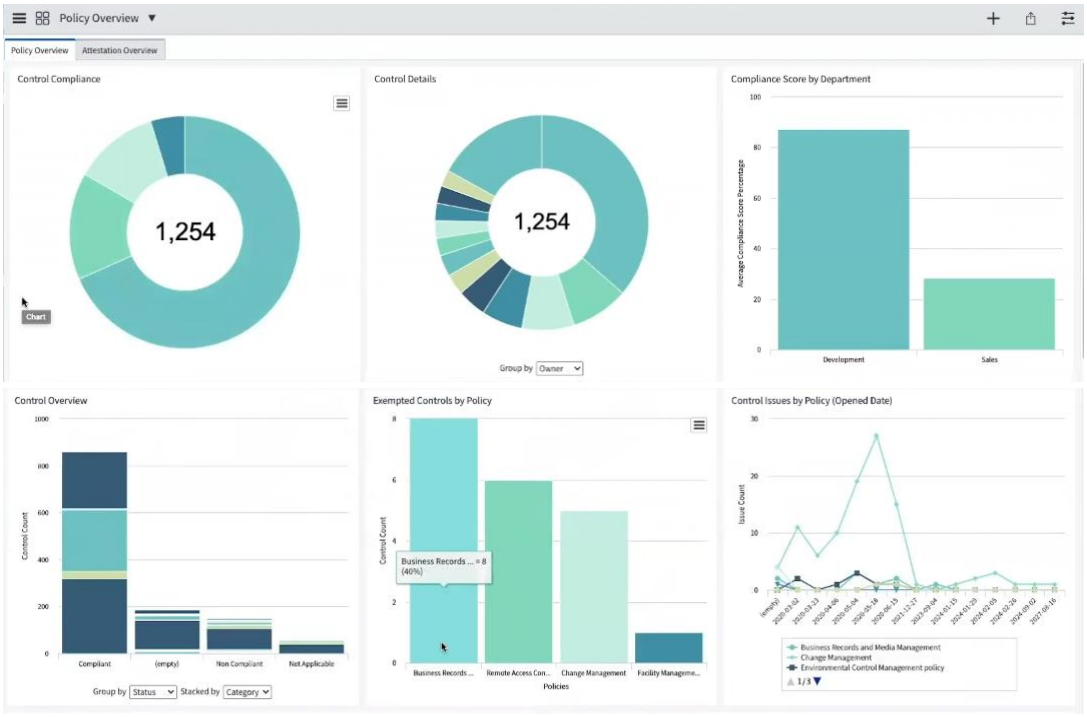


Figura 5.21 - Dashboard de policy no ServiceNow

Tendo em conta que uma das vantagens que a abordagem GRC fornece às empresas que a implementam é a de facilitação de todo o processo de auditoria, o *software* ServiceNow inclui ainda *dashboard* relativos ao compromisso de auditoria, estes encontram-se apresentados na Figura 5.22.

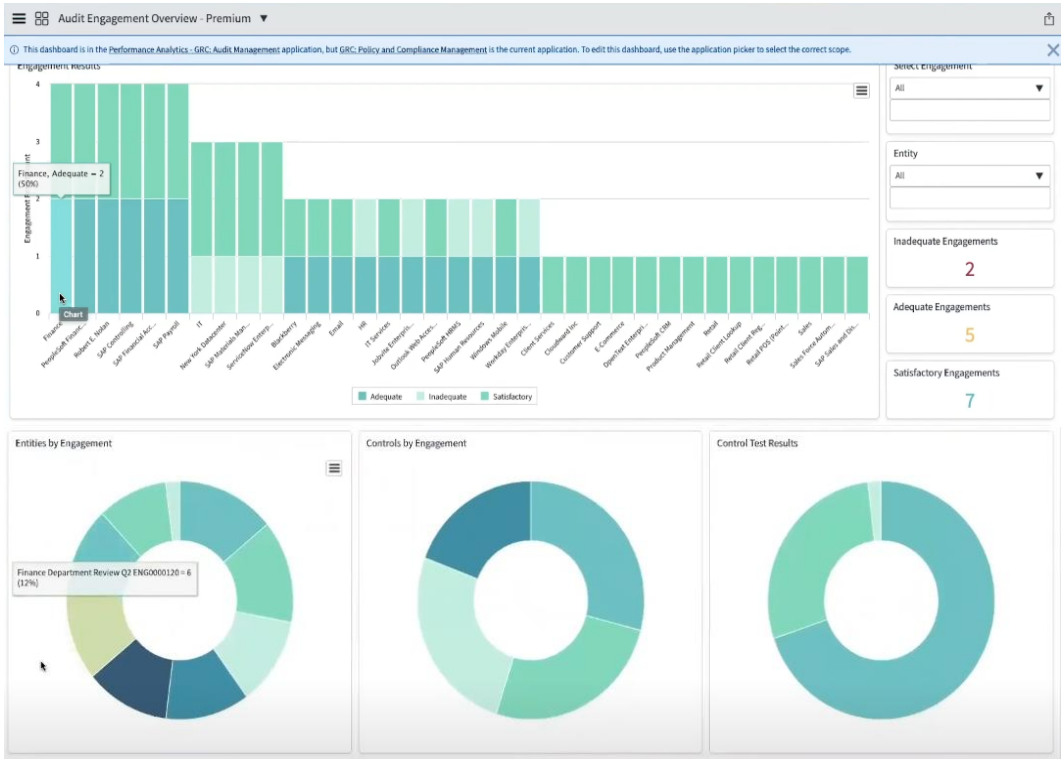


Figura 5.22 - Dashboard de audit engagement no ServiceNow

A auditoria verifica se os controlos que a empresa possui estão em correto funcionamento. Os controlos são testados de duas maneiras diferentes, a primeira assenta no teste de adequação do *design* do controlo e a segunda na eficácia da aplicação ou desempenho do mesmo. Frequentemente as descobertas dos auditores definem que o *design* dos controlos é apropriado, no entanto, estes não foram implementados corretamente. É mais comum obter-se falhas no lado operacional de um controlo do que na conceção desse mesmo controlo. A *overview* do compromisso de auditoria no ServiceNow é, basicamente, o *status* atual da auditoria. Esta secção mostra o estado atual de como os vários processos e atividades organizacionais estão a correr, a sua adequação e satisfação do seu propósito intrínseco, sendo que a maior parte do trabalho, quando se trata de uma auditoria, é feito através da colocação de questões operativas.

Por fim é possível verificar a eficácia geral obtida pelo funcionamento conjunto dos módulos do ServiceNow utilizados. Apesar de ser fazível a gestão dos riscos sem a interligação com os controlos e auditoria, a menos que seja executada a gestão de políticas e conformidade, não é possível verificar quais controlos estão alocados à mitigação de riscos e, consequentemente, impossibilita a realização de ações de melhoria ou correção na fonte do problema. É também concretizável a utilização do *software* apenas para gestão de conformidade, ou seja, sem a gestão dos riscos e auditoria, no entanto, mais uma vez, esta aplicação parcial incapacita o ServiceNow de verificar a aplicabilidade operacional dos controlos e a atenuação, em termos de impacto de exposição e no negócio, que estes podem infligir no aspeto financeiro do risco. A implementação conjunta dos dois módulos permite uma apreciação momentânea do que é feito diariamente, quão bem é feito e o dinheiro economizado ao fazê-lo.

6. CONCLUSÕES

Em virtude do objetivo definido para a presente dissertação, que consta no desenvolvimento de uma metodologia que permita assegurar a correta implementação da abordagem GRC, considera-se que este foi atingido. A metodologia desenvolvida assente na aplicação da FMEA com integração de *skills* de automação pelo *software* ServiceNow permitiu a aplicação fluída da abordagem em questão. Tal afirmação é suportada maioritariamente devido aos resultados obtidos, em termos do cálculo do risco, RPN, anteriormente e posteriormente à execução de ações de melhoria e correção. Uma vez que estes representam o sucesso do objetivo definido, é intenção da organização expandir a metodologia desenvolvida na presente dissertação aos restantes departamentos e empresas do Grupo EDP, como planeado e agora evidenciado como uma medida eficaz e eficiente.

Ao atuar praticamente como uma medida preventiva, a FMEA fornece uma abordagem sistemática de direcionamento de ações de melhoria necessárias a fim de reduzir o risco, com o objetivo de corrigir antecipadamente as causas de potenciais falhas de um processo. Esta aplicabilidade é fulcral na implementação da estratégia de gestão do risco em TI decidida pelo Grupo EDP visto que, para qualquer risco identificado cuja resposta pretende ser a de mitigação, é de extrema importância a reflexão lógica sobre as apropriadas ações de correção ou melhoria necessárias à resolução da causa do problema em si, ou seja, da causa do potencial modo de falha tendo em conta a dimensão dos possíveis efeitos consequentes à mesma. Acrescenta-se que a automatização de todo este processo, recorrente ao *software* ServiceNow, habilita o controlo e monitorização, em tempo real, da exposição ao risco, elevando assim as vantagens anteriormente mencionadas pois a avaliação da situação atual, como os cálculos do RPN, é feita ao segundo. A implementação automatizada de toda a abordagem GRC permite ainda priorizar a resposta aos riscos mais críticos através do programa GRC unificado, ou seja, através da utilização interligada temporalmente entre os diferentes módulos do *software*, isto leva a uma redução da carga geral dos colaboradores pertencente à equipa de segurança visa a existência de fluxos de trabalhado consistentes e devido à própria automação configurada. Também o processo de tomada de decisão é facilitado com o programa único de gestão integrada. Através da análise dos *dashboards* contruídos automaticamente pelo ServiceNow, é possível obter informações relevantes sobre as áreas de alto risco, não conformidades, *status* dos

vendedores e descobertas de auditoria significativas. Desta forma, ao avaliar o contexto e impacto do negócio, a priorização de atividades, a comunicação visual e as decisões estratégicas são facilitadas. Consequentemente ocorre aumento de desempenho consistente multifuncional, impulsionando assim a produtividade e a redução de falhas, dando, novamente, às equipas, mais tempo de concentração em tarefas de maior valor através desta redução de carga geral de trabalho graças à implementação da abordagem GRC.

Considera-se, ainda, que a presente implementação GRC bem-sucedida deu resposta às metas definidas nos passos preliminares do projeto, metas estas de resposta às limitações encontradas incialmente na gestão do risco no Grupo EDP, fortalecendo, assim, os contributos que o presente caso prático deixou à organização.

Contornou-se a limitação da centralização da informação referente às TI, tal foi obtido e mantido através do reenforço da utilização, por parte de toda a equipa de Security & Risk, do mesmo *software* de trabalho da informação relacionada ao tema, *software* ServiceNow. Esta transição de métodos de trabalho dentro da gestão do risco em TI foi suave devido às elucidações realizadas onde, não só os benefícios da transição foram enfatizados, como também se procedeu à demonstração de todos os serviços automatizados descendentes da mesma. Estes últimos impedem a repetição de diversas atividades manuais pelo que agilizam diversos procedimentos da responsabilidade de vários membros da equipa. Este contributo para o Grupo EDP permitiu ainda a redução temporal de todos os processos de aquisição e partilha de informação dentro da DGU. Acrescenta-se ainda a uniformização dos dados concretos existentes, um exemplo desta situação é em termos dos métodos de avaliação do risco. À priori à implementação prática da metodologia desenvolvida sobre a adaptação da abordagem GRC, os sistemas avaliativos do risco encontravam-se assentes apenas em termos qualitativos sem escalabilidade ou forma de comparação, pelo que, as percepções de diferentes colaboradores poderiam entrar em choque criando assim valores pouco representativos e muitas vezes irrealistas. A metodologia desenvolvida possibilita a avaliação qualitativa segundo valores quantitativos como valores financeiros e probabilisticos, consequentemente, a ponderação torna-se, assim, confiável visto que todos os avaliadores compreendem as bases e o significado de cada nível das escalas.

Uma outra limitação enunciada no início do projeto encontra-se na falta de interligação e associação entre controlos, riscos e conformidade regulamentar do Grupo EDP. Igualmente à limitação anterior, também esta foi ultrapassada. A visão holística desejada encontra-se, neste momento, implementada e automatizada no *software* ServiceNow. Este permite a coneção da informação de forma a impedir a existência de dados duplicados ou inválidos. O processo de automatização que a utilização do *software* implica leva a um encadeamento realista e pertinente da informação relativo, não só ao risco, como também aos controlos respetivos originados pelos documentos que determinam a conformidade para a empresa.

Ainda como contributo para o Grupo EDP, a implementação descrita na presente dissertação proporciona a presença garantida e funcional de monitorização constante dos ativos e entidades. Tal ocorre através do acompanhamento contínuo sobre o desempenho dos ativos e entidades adotadas através de índices de *performance*. Como acrescente aos índices de *performance*, a metodologia desenvolvida cujo propósito incide numa implementação correta da abordagem GRC consente ainda a designação de responsabilidade sobre riscos e entidades.

Deste modo, os colaborabores encarregues sobre riscos, ativos ou documentação de conformidade encontram-se a par das últimas atualizações sobre os fatores sob sua responsabilidade. Da mesma maneira, os responsáveis mantêm qualquer informação atualizada relacionada com possíveis ações de resposta a diversos estados das entidades ou riscos e quaisquer *updates* efetuados, visto que, os mesmos acontecem no *software* ServiceNow.

A junção dos factores de monitorização ao segundo, ou seja, atualização automática constante, e de interligação sobre a informação existente, trabalhada, renovada e criada, viabiliza uma visão uniformizada, acertada e verdadeira da gestão do risco do Grupo EDP. Consequentemente, é assim possível obter a noção do nível de conformidade legal e nível de risco e do estado atual da organização para diversas frentes incluindo, aquando da finalização da expansão do projeto aos restantes departamentos, todas as geografias.

A agregação de todas as vantagens obtidas concede à área de segurança de TI a oportunidade de aplicar ferramentas estratégicas de forma a conquistar metas delineadas para a empresa. Esta possibilidade encontra-se otimizada e facilitada por mérito da automação, que se traduz numa eficácia operacional dos controlos, neste momento existente em diversos processos precedentemente somente manuais. Concede ainda a conveniência de uma gestão transparente dos ativos com a oportunidade de criação de inventários dos recursos tecnológicos usados pela organização, como foi feito, e controlar constantemente o seu funcionamento.

Ao longo do estudo descrito e desenvolvido para atingir o objetivo da dissertação colocada na gestão do risco em TI, para além dos contributos adquiridos, foram encontrados robustecimentos da metodologia, do sistema e das suas possíveis aplicações.

Um passo interessante aplicado e que resultou em grande valor acrescentado à metodologia desenvolvida na presente dissertação, encontra-se na vertente da "Efetividade dos Controlos" presente na secção "CHECK" da metodologia FMEA. A verificação da qualidade dos controlos considera-se essencial dada a sua diferença relativa ao fator de avaliação da "Deteção" dos controlos. A capacidade de detetar uma falha não tem que estar intrínsecamente análoga à efetividade do controlo de deteção ou prevenção da mesma, sendo que, o último pode depender de numerosos coeficientes de implementação e manutenção do próprio controlo. Dado isto, a confirmação da efetividade dos controlos gerada pela configuração do *software* ServiceNow, em modo de percentagem, permite a noção consciente dos possíveis efeitos da inexistência de controlos funcionais, como eventuais fraudes ou mesmo perdas para a empresa. Com esta informação pertinente e fulcral, as ações de correção e melhoria podem estar mais focadas no problema real do potencial modo de falha em questão, não aderindo, assim, a soluções improváveis e mal direcionadas à causa-raiz. Devido a tal considera-se interessante o desenvolvimento deste parâmetro da metodologia FMEA numa visão quantitativa. Apesar de não ser um método tradicional de aplicação da FMEA devido a prováveis impossibilidades de automação viável ou de melhor verificação da efetividade de controlos, seja esta não só qualitativa, a presente dissertação demonstra a eficiência prática do mesmo.

Incorpora-se, por fim, como proposta para trabalhos futuros, mais precisamente para a expansão do procedimento ao Grupo EDP como totalidade, a inclusão do parâmetro de avaliação da "Deteção" na configuração da avaliação realizada no *software* ServiceNow. Neste

momento existe a possibilidade de seleção, dentro da estruturação e composição de um controlo, módulo *policy&compliance*, do propósito do mesmo, ou seja, seleção entre controlo preventivo ou controlo de deteção. No entanto, não ocorre a avaliação específica ao nível de deteção deste. Apesar da existência maioritária de controlos de prevenção dentro do Grupo EDP, o parâmetro de avaliação de deteção aplicado na metodologia FMEA, mostrou-se imensamente útil na decisão e planeamento de atividades de melhoria e correção. Através da avaliação dos três parâmetros defendidos pela metodologia FMEA, "Ocorrência", "Gravidade" e "Deteção" é possível definir o caminho mais concreto que as ações de melhoria devem seguir para fornecer uma resposta específica aos níveis de avaliação recebidos.

REFERÊNCIAS BIBLIOGRÁFICAS

Aven, T. (2012). The risk concept—Historical and recent development trends. *Reliability Engineering & System Safety*, *99*, 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Aven, T. (2013). On Funtowicz and Ravetz's «decision stake-system uncertainties» structure and recently developed risk perspectives. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *33*(2), 270–280. https://doi.org/10.1111/j.1539-6924.2012.01857.x

Aven, T. (2019). The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, *39*(6), 1196–1203. Scopus. https://doi.org/10.1111/risa.13247

Aven, T., & Krohn, B. S. (2014). A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering & System Safety*, *121*, 1–10. https://doi.org/10.1016/j.ress.2013.07.005

Balke, N. (2014, Abril 17). ebook: PDF⋙ Risk and Decision Analysis in Projects (Cases in project and program management series) by John R. Schuyler. *ebook*. https://nerisalke.blogspot.com/2014/04/pdf-risk-and-decision-analysis-in.html

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Barafort, B., Mesquida, A.-L., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces*, *60*, 57–66. https://doi.org/10.1016/j.csi.2018.04.010

Ben-Daya, M., & Raouf, A. (1996). A revised failure mode and effects analysis model. *International Journal of Quality and Reliability Management*, *13*(1), 43–47. Scopus. https://doi.org/10.1108/02656719610108297

Boral, S. (2021). An integrated interval type-2 fuzzy sets and multiplicative half quadratic programming-based MCDM framework for calculating aggregated risk ranking results of failure modes in FMECA. *Process Safety and Environmental Protection*, 29.

Bristow, D., Bristow, M., Fang, L., & Hipel, K. (2013, Junho 1). *Evolution of Cities and Urban Resilience through Complex Adaptation and Conflict Resolution*.

Chou, D. C. (2007). An investigation into IS outsourcing success: The role of quality and change management. *International Journal of Information Systems and Change Management*, *2*(2), 190. https://doi.org/10.1504/IJISCM.2007.015119

Chou, D. C. (2015a). Cloud computing: A value creation model. *Computer Standards & Interfaces*, *38*, 72–77. https://doi.org/10.1016/j.csi.2014.10.001

Chou, D. C. (2015b). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, *42*, 137–142. https://doi.org/10.1016/j.csi.2015.06.005

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). Cloud security is not (just) virtualization security: A short paper. *Proceedings of the 2009 ACM workshop on Cloud computing security*, 97–102. https://doi.org/10.1145/1655008.1655022

Cicek, K., & Celik, M. (2013). Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. *Safety Science*, *51*(1), 6–10. https://doi.org/10.1016/j.ssci.2012.06.003

John R. Vacca (2017). Computer and Information Security Handbook. *Network Security* (11), 4. https://doi.org/10.1016/S1353-4858(17)30090-9

INTEGRITY. (2021). *Consultoria Cibersegurança.* Obtido 14 de Julho de 2021, de https://www.integrity.pt/pt/consultoria.html

CPA. (2009). Virtualization Security Assessment. *Information Security Journal: A Global Perspective*, *18*(3), 124–130. https://doi.org/10.1080/19393550902791440

Crovini, C., Ossola, G., & Britzelmaier, B. (2021). How to reconsider risk management in SMEs? An Advanced, Reasoned and Organised Literature Review. *European Management Journal*, *39*(1), 118–134. https://doi.org/10.1016/j.emj.2020.11.002

Jornal Expresso. (2021). *EDP alvo de ataque informático*. Obtido 20 de Setembro de 2021, de https://expresso.pt/economia/2020-04-13-EDP-alvo-de-ataque-informatico

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, *2011*(1), 5–7. https://doi.org/10.1016/S1361-3723(11)70005-7

EDP. (2021). Fatores de Risco. Obtido 14 de Março de 2021, de https://ri.edp.com.br/pt-br/informacoes-aos-investidores/fatores-de-risco/

Fazlida, M. R. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, 6.

Fikri, M. A., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Filz, M.-A., Langner, J. E. B., Herrmann, C., & Thiede, S. (2021). Data-driven failure mode and effect analysis (FMEA) to enhance maintenance planning. *Computers in Industry*, *129*, 103451. https://doi.org/10.1016/j.compind.2021.103451

Fraser, J. R. S., Quail, R., & Simkins, B. J. (2021). Questions that are asked about enterprise risk management by risk practitioners. *Business Horizons*, S0007681321000653. https://doi.org/10.1016/j.bushor.2021.02.046

Gargama, H., & Chaturvedi, S. K. (2011). Criticality assessment models for failure mode effects and criticality analysis using fuzzy logic. *IEEE Transactions on Reliability*, *60*(1), 102–110. Scopus. https://doi.org/10.1109/TR.2010.2103672

Gartner. (2021). *Magic Quadrant for IT Risk Management*. Obtido 22 de Maio de 2021, de https://www.gartner.com/doc/reprints?id=1-1ZHQ1JNZ&ct=200717&st=sb

Garvey, P. (2021). Analytical Methods for Risk Management. *Statistics: A Series of Textbooks and Monographs*. Obtido 27 de Setembro de 2021, de https://www.academia.edu/11855548/Analytical_Methods_for_Risk_Management

EDP (2021). *Governo da Sociedade - Gestão de Risco*. Obtido 14 de Março de 2021, de https://www.edp.com/pt-pt/investidores/governo-da-sociedade/gestao-de-risco

Gewald, H., & Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information and Management*, *46*(4), 249–257. Scopus. https://doi.org/10.1016/j.im.2009.03.002

Grey, S. (1995). *Practical risk assessment for project management*. Wiley.

Hassan, S., Wang, J., Kontovas, C., & Bashir, M. (2022). Modified FMEA hazard identification for cross-country petroleum pipeline using Fuzzy Rule Base and approximate reasoning. *Journal of Loss Prevention in the Process Industries*, *74*, 104616. https://doi.org/10.1016/j.jlp.2021.104616

Hohan, A. I. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, 8.

Hunt, R. (2014). Why governance, risk and compliance projects fail – and how to prevent it. *Computer Fraud & Security*, *2014*(6), 5–7. https://doi.org/10.1016/S1361-3723(14)70499-3

INTEGRITY. (2021). *Serviços de Cibersegurança*. Obtido 14 de Julho de 2021, de https://www.integrity.pt/pt/

ISO 27001. (2013). ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements (Segunda edição de 1 de Outubro de 2013).

ISO 31000:2009. (2009). *Risk management - Principles and guidelines* (EN, 1st Edition – outdated, revised in 2018).

Jaderi, F., Ibrahim, Z. Z., & Zahiri, M. R. (2019). Criticality analysis of petrochemical assets using risk based maintenance and the fuzzy inference system. *Process Safety and Environmental Protection*, *121*, 312–325. https://doi.org/10.1016/j.psep.2018.11.005

Jiang, L., Sun, X., Ji, C., Kabene, S. M., & Abo Keir, M. Y. (2021). PDCA cycle theory based avoidance of nursing staff intravenous drug bacterial infection using degree quantitative evaluation model. *Results in Physics*, *26*, 104377. https://doi.org/10.1016/j.rinp.2021.104377

Jianxing, Y., Shibo, W., Haicheng, C., Yang, Y., Haizhao, F., & Jiahao, L. (2021). Risk assessment of submarine pipelines using modified FMEA approach based on cloud model and extended VIKOR method. *Process Safety and Environmental Protection*, S0957582021005206. https://doi.org/10.1016/j.psep.2021.09.047

Jones, E. C., Parast, M. M., & Adams, S. G. (2010). A framework for effective Six Sigma implementation. *Total Quality Management & Business Excellence*, *21*(4), 415–424. https://doi.org/10.1080/14783361003606720

Kalathil, M. J. (2020). Failure mode effect and criticality analysis using dempster shafer theory and its comparison with fuzzy failure mode effect and criticality analysis: A case study applied to LNG storage facility. *Process Safety and Environmental Protection*, 12.

Klein Jr., V. H., & Reilley, J. T. (2021). The temporal dynamics of enterprise risk management. *Critical Perspectives on Accounting*, 102363. https://doi.org/10.1016/j.cpa.2021.102363

Kremljak, Z., & Kafol, C. (2014). Types of Risk in a System Engineering Environment and Software Tools for Risk Analysis. *Procedia Engineering*, *69*, 177–183. https://doi.org/10.1016/j.proeng.2014.02.218

Kumar, M. (2020). System failure probability evaluation using fault tree analysis and expert opinions in intuitionistic fuzzy environment. *Journal of Loss Prevention in the Process Industries*, 15.

Laine, V., Goerlandt, F., Banda, O. V., Baldauf, M., Koldenhof, Y., & Rytkönen, J. (2021). A risk management framework for maritime Pollution Preparedness and Response: Concepts, processes and tools. *Marine Pollution Bulletin*, *171*, 112724. https://doi.org/10.1016/j.marpolbul.2021.112724

Landquist, H., Hassellöv, I.-M., Rosén, L., Lindgren, J. F., & Dahllöf, I. (2013). Evaluating the needs of risk assessment methods of potentially polluting shipwrecks. *Journal of Environmental Management*, *119*, 85–92. https://doi.org/10.1016/j.jenvman.2012.12.036

Li, H., Díaz, H., & Guedes Soares, C. (2021). A failure analysis of floating offshore wind turbines using AHP-FMEA methodology. *Ocean Engineering*, *234*, 109261. https://doi.org/10.1016/j.oceaneng.2021.109261

Li, Q., Yuan, H., Jing, B., Liu, Z., Li, W., Cheng, J., Gong, B., & Sun, J. (2010). Theoretical study of halogen bonding between FnH3−nCBr (n=0, 1, 2, 3) and HMgH. *Journal of Molecular Structure*, 4.

Li, S.-H., Yen, D. C., Chen, S.-C., Chen, P. S., Lu, W.-H., & Cho, C.-C. (2015). Effects of virtualization on information security. *Computer Standards & Interfaces*, *42*, 1–8. https://doi.org/10.1016/j.csi.2015.03.001

Liu, H.-C., Liu, L., Bian, Q.-H., Lin, Q.-L., Dong, N., & Xu, P.-C. (2011). Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory. *Expert Systems with Applications*, *38*(4), 4403–4415. https://doi.org/10.1016/j.eswa.2010.09.110

Liu, H.-C., Wang, L.-E., Li, Z., & Hu, Y.-P. (2019). Improving Risk Evaluation in FMEA With Cloud Model and Hierarchical TOPSIS Method. *IEEE Transactions on Fuzzy Systems*, *27*(1), 84–95. https://doi.org/10.1109/TFUZZ.2018.2861719

John. (2001). *Analyzing and managing risky investments* (1st ed.). J.M. Campbell.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

Meriah, I., & Arfa Rabai, L. B. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, *160*, 85–92. https://doi.org/10.1016/j.procs.2019.09.447

Mesquida, A.-L., Mas, A., Feliu, T. S., & Arcilla, M. (2014). MIN-ITs: A framework for integration of IT management standards in mature environments. *International Journal of Software Engineering and Knowledge Engineering*, *24*(6), 887–908. Scopus. https://doi.org/10.1142/S0218194014400026

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution and Logistics Management*, *34*(5), 434–456. Scopus. https://doi.org/10.1108/09600030410545463

O'Leary, M. (1990). The mainframe doesn't work here anymore. *CIO*, *6*(6), 77–79. Scopus.

Perçin, S. (2008). Fuzzy multi-criteria risk-benefit analysis of business process outsourcing (BPO). *Information Management & Computer Security*, *16*(3), 213–234. https://doi.org/10.1108/09685220810893180

Pillay, A., & Wang, J. (2003). Modified failure mode and effects analysis using approximate reasoning. *Reliability Engineering & System Safety*, *79*(1), 69–85. https://doi.org/10.1016/S0951-8320(02)00179-5

Pouyakian, M. (2021). A comprehensive approach to analyze the risk of floating roof storage tanks. *Process Safety and Environmental Protection*, 26.

Ramalingam, D., Arun, S., & Anbazhagan, N. (2018). A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM. *Procedia Computer Science*, *134*, 365–370. https://doi.org/10.1016/j.procs.2018.07.197

Rezaei Soufi, H., Esfahanipour, A., & Akbarpour Shirazi, M. (2021a). A quantitative approach for analysis of macroeconomic resilience due to socio-economic shocks. *Socio-Economic Planning Sciences*, 101101. https://doi.org/10.1016/j.seps.2021.101101

Rezaei Soufi, H., Esfahanipour, A., & Akbarpour Shirazi, M. (2021b). Risk reduction through enhancing risk management by resilience. *International Journal of Disaster Risk Reduction*, *64*, 102497. https://doi.org/10.1016/j.ijdrr.2021.102497

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273. https://doi.org/10.1016/j.ejor.2014.09.055

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2018). Building organizational resilience in the face of multiple disruptions. *International Journal of Production Economics*, *197*, 63–83. https://doi.org/10.1016/j.ijpe.2017.12.009

Sangpikul, A. (2017). Implementing academic service learning and the PDCA cycle in a marketing course: Contributions to three beneficiaries. *Journal of Hospitality, Leisure, Sport & Tourism Education*, *21*, 83–87. https://doi.org/10.1016/j.jhlste.2017.08.007

Scipioni, A., Saccarola, G., Centazzo, A., & Arena, F. (2002). FMEA methodology design, implementation and integration with HACCP system in a food company. *Food Control*, *13*(8), 495–501. https://doi.org/10.1016/S0956-7135(02)00029-4

Shi, Y. (2007). Today's Solution and Tomorrow's Problem: The Business Process Outsourcing Risk Management Puzzle. *California Management Review*, *49*(3), 27–44. https://doi.org/10.2307/41166393

Song, M. H., & Fischer, M. (2020). Daily plan-do-check-act (PDCA) cycles with level of development (LOD) 400 objects for foremen. *Advanced Engineering Informatics*, *44*, 101091. https://doi.org/10.1016/j.aei.2020.101091

Song, Q. (2021). The application of cloud model combined with nonlinear fuzzy analytic hierarchy process for the safety assessment of chemical plant production process. *Process Safety and Environmental Protection*, 11.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201–218. https://doi.org/10.1016/j.ssci.2016.06.015

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Vidmar, P., & Perkovič, M. (2018). Safety assessment of crude oil tankers. *Safety Science*, *105*, 178–191. https://doi.org/10.1016/j.ssci.2018.02.009

Vinha, N. (2021). *EDP alvo de ataque informático que bloqueou sistemas de atendimento aos clientes*. Observador. Obtido 20 de Setembro de 2021, de https://observador.pt/2020/04/13/edp-alvo-de-ataque-informatico-que-bloqueou-sistemas-de-atendimento-aos-clientes/

Wang, L., Yan, F., Wang, F., & Li, Z. (2021). FMEA-CM based quantitative risk assessment for process industries—A case study of coal-to-methanol plant in China. *Process Safety and Environmental Protection*, *149*, 299–311. https://doi.org/10.1016/j.psep.2020.10.052

Yazdi, M., Nedjati, A., Zarei, E., & Abbassi, R. (2020). A reliable risk analysis approach using an extension of best-worst method based on democratic-autocratic decision-making style. *Journal of Cleaner Production*, *256*, 120418. https://doi.org/10.1016/j.jclepro.2020.120418

Zhang, D., Yan, X. P., Yang, Z. L., Wall, A., & Wang, J. (2013). Incorporation of formal safety assessment and Bayesian network in navigational risk estimation of the Yangtze River. *Reliability Engineering & System Safety*, *118*, 93–105. https://doi.org/10.1016/j.ress.2013.04.006

Zhang, Y., Liu, S., Tan, J., Jiang, G., & Zhu, Q. (2018). Effects of risks on the performance of business process outsourcing projects: The moderating roles of knowledge management capabilities. *International Journal of Project Management*, *36*(4), 627–639. https://doi.org/10.1016/j.ijproman.2018.02.002

Zohuri, B., & McDaniel, P. (2021). Appendix A - Plan-do-check-act (PDCA) cycle. Em B. Zohuri & P. McDaniel (Eds.), *Introduction to Energy Essentials* (pp. 549–558). Academic Press. https://doi.org/10.1016/B978-0-323-90152-9.00015-3

A.
ANEXOS

PLAN		DO									CHECK	ACT		Resultados			
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos	Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
Função	Potenciais Modos de Falha					Prev.	Det.										
Controlar Acessos	O acesso à informação, aos sistemas e recursos de TI do Grupo EDO, e aos seus processos de Negócio não é controlado com base nos requisitos de Segurança da Informação e de Negócio, bem como nos requisitos de legislação e regulamentação	Acesso ilegítimo	1	Existência de controlos de acesso ineficientes devido a incoerências com a legislação	2	Procedimentar o controlo de acesso à informação	-	5	10	Sistemas, recursos de TI e processos de Negócio	60%	Motivar a resposta aos indicadores	Aumentar a regularidade das reuniões de equipa	1	1	5	5
						Procedimentar o controlo de acesso à informação					100%	-	-				
	O acesso aos sistemas e aplicações não é restringido aos utilizadores autorizados, não é garantida a utilização de mecanismos de autenticação adequados e registo dos acessos realizados	Acesso ilegítimo	3	Acesso ilegítimo por incorreta restrição de utilizadores	1	-	Sistema de deteção de credenciais inexistentes	1	3	Sistemas e equipamentos	100%	-	-	3	1	1	3
							Autenticação				100%	-	-				
	As regras de controlo de acesso não têm em consideração as regras definidas para a partilha da Informação	Não aplicável	-	Não aplicável	-	Não aplicável	Não aplicável	-	-	-	-	-	-	-	-	-	-
	A Norma de controlo de acessos não se encontra aprovada	Falta de documentação	1	Falta de complience da norma controlo de acessos	1	-	Processo de aprovação documentacional	1	1	Documento normativo	100%	-	-	1	1	1	1
	Esta Norma não é revista anualmente, ou sempre que ocorra uma mudança (legislação, orientação interna, etc.) que o justifique	Documentação desatualizada	1	Falta de complience da norma controlo de acessos	1	Notificações de revisão	Processo de revisão documentacional anual	1	1	Documento normativo	100%	-	-	1	1	1	1
	Os utilizadores, internos e externos, não se encontram informados das regras estabelecidas nesta Norma	Acessos indevidos	2	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	2	-	Formações sobre Controlo de acessos	4	16	Documento normativo	40%	Testar os conhecimentos	Construção de apresentações de aprendizagem diretas e práticas	2	1	2	4
	A arquitetura de segurança para o controlo de acessos aos serviços de rede do Grupo EDP não tem aprovação da área de Segurança da Informação	Falta de documentação	1	Existência de controlos de acesso ineficientes por falta de aprovação	1	Aprovação da arquitetura de segurnaça	Controlo automático de evidência de aprovação prévia	1	1	Sistemas, recursos de TI e processos de Negócio	100%	-	-	1	1	1	1
	Os terminais que permitem o acesso aos serviços de rede de utilização interna não estão protegidos por mecanismos de controlo de acessos	Acesso não autorizado	2	Comprometimento da rede devido à falta de controlos de acesso	1	Proteger terminais de acesso	Mecanismos de controlo de acesso a rede de comunicações	1	2	Aplicações	100%	-	-	2	1	1	2
	Os colaboradores e as entidades utilizam o acesso à rede partir de redes informáticas exteriores	Acessos não controlados	1	Comprometimento da rede devido à utilização indevidde redes não autorizadas	1	-	Proibição automática de acesso acessos através de redes informáticas exteriores	1	1	Sistemas e equipamentos	100%	-	-	1	1	1	1
	Os acessos à Internet a partir da rede informática e terminais do Grupo EDP não utilizam mecanismos e ferramentas conFiguradas e geridas de acordo com as definições da DGU	Comprometimento da rede informática e dos terminais do Grupo EDP	1	Comprometimento da rede devido à falta de controlos de acesso	2	Dispor de ferramentas de deteção de intrusões	-	5	10	Rede informática	65%	Mecanismos de proteção contra intrusões	-	1	2	2	4
	Os colaboradores e as entidades externas que acedem à Internet a partir da rede informática e terminais do Grupo EDP não são responsáveis por respeitar os direitos de propriedade intelectual aplicáveis aos conteúdos acedidos	Usurpação de propriedade intelectual terceira	2	Usurpação de propriedade intelectual do grupo EDP	2	-	-	5	20	Rede informática	0%	-	Formações sobre direitos de propriedade intelectual	2	1	5	10
	O Grupo EDP não aplica o direito de, no permitido pela moldura legal, sem aviso prévio, limitar o acesso total ou parcial à Internet a partir da rede informática e terminais do Grupo EDP	Atividades indevidas ou acesso a sites maliciosos realizados da rede informática e terminais do Grupo EDP	1	Comprometimento da rede devido à utilização indevida da rede informática	4	-	-	5	20	Rede informática	0%	-	Limitar acessos automaticamente	1	1	1	1
	O acesso à informação não se encontra restringido com base nos critérios estabelecidos pelo Negócio e em concordância com o definido nesta Norma	Acesso a informações não necessárias para a realização das funções	1	Acesso ilegítimo por incorreta restrição de utilizadores	1	Restrição do acesso à informação	-	5	5	Sistemas, recursos de TI e processos de Negócio	80%	-	-	1	1	5	5

PLAN		DO									CHECK	ACT		Resultados			
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos	Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
Função	Potenciais Modos de Falha					Prev.	Det.										
	Falta de permissões de acesso e operações autorizadas sobre a informação, como por exemplo: escrever, ler, apagar ou executar	Inexistência de segregação de acessos/ atividades	1	Acções acidentais ou repúdio de acções sobre informação por controlo de acessos indevido	3	Definir procedimentos de registos de ações que permitem auditar as operações	Monitorizar e rever as permissões e operações sobre a informação	1	3	Sistemas, equipamentos e aplicações	60%	Motivar a resposta aos indicadores	-	1	2	1	2
	Acessos sem controlo a outras aplicações	Inexistência de segregação de acessos/ atividades	3	Acesso ilegítimo por incorreta restrição de utilizadores	4	-	-	5	60	Aplicações	0%	-	Restringir automaticamente acessosa outras aplicações segundo as regras normativas do Grupo EDP	3	1	2	6
	Não se encontra determinado o tipo de dados e/ou informação que pode ser acedido por determinado utilizador	Inexistência de segregação de acessos/ atividades	2	Acesso ilegítimo por incorreta restrição de utilizadores	5	-	-	5	50	Informação	0%	-	Determinar e efetuar a classificação da informação por tipo de colaborador	2	3	5	30
	Informação ilimitada nos outputs	Inexistência de segregação de acessos/ atividades	4	Inexistência de segregação de acessos/ atividades devido à falta de mecanismos de controlo	1	Limitar informação nos outputs	-	5	20	Sistemas, equipamentos e aplicações	100%	-	-	4	1	5	20
	É revelada informação sobre os sistemas a quem tenta aceder até que o *logon* esteja concluído ou é mostrada a password durante a respetiva introdução	Revelação de informações sobre sistema a ser acedido e a password de acesso	5	Revelação de informações sobre o sistema devido à inexistência de mecanismos de ocultação	1	Mascaramento em ambientes pré-produtivos	-	5	25	Sistemas e recursos de TI	100%	-	-	5	1	5	25
						Ocultar informações durante logon					100%	-	-				
	Durante o processo de *logon* é disponibilizada informação que facilite o acesso de utilizadores não autorizados	Revelação de informações sobre sistema a ser acedido e a password de acesso	5	Revelação de informações sobre o sistema devido à inexistência de mecanismos de ocultação	1	Mascaramento em ambientes pré-produtivos	Impedir automaticamente acesso indevido	1	5	Sistemas, equipamentos e aplicações	100%	-	-	5	1	1	5
	A Informação de *logon* não é validada como um todo e, caso ocorra uma situação de erro, o sistema indica que parte da Informação está errada	Revelação de mensagens de erro contendo informações que podem ser utilizadas para fins maliciosos	5	Comprometimento do *logon* por validação insegura	1	Logon é validado como um todo	-	5	25	Sistemas, equipamentos e aplicações	100%	-	-	5	1	5	25
	As tentativas de *logon* sem sucesso são ilimitadas em número	*Logon* bem-sucedido através de *Brute Force Attack*	5	Comprometimento do *logon* por validação insegura	2	Limitar as tentativas de logon	Detetar tipo de tentativas maliciosas	2	50	Sistemas e recursos de TI	20%	Estabelecer um número limite geral para todo o Grupo EDP	Programar deteção dos vários tipos de tentativas de *logon* maliciosas	5	1	1	5
	As tentativas de *logon* não são registadas, quer sejam ou não bem-sucedidas	Repúdio de ações	1	Repúdio de ações devido à conFiguração inadequada dos mecanismos de *logon*	1	Registo de todas as tentativas de acesso	.	5	5	Sistemas, equipamentos e aplicações	40%	Garantir formalmente o registo de todas as tentativas de acesso	Verificar regularmente o cumprimento do princípio	1	1	2	2
						Integração com o SIEM					100%						
	Não se encontra garantido que a operação de *logon* não envia as credenciais de acesso de forma desprotegida através da rede	Comprometimento de credenciais de acesso	4	Comprometimento de credenciais de acesso devido à utilização de protocolos inseguros aplicáveis aos sistemas e aplicações	2	-	Operação de logon protege e deteta envios de credenciais	1	8	Rede informática	100%	-	-	4	2	1	8
	Não se encontra visível a data e hora do último *logon* com sucesso	Repúdio de ações	1	Repúdio de ações devido à conFiguração inadequada dos mecanismos de *logon*	4	Apresentação da data e hora do último logon	-	5	20	Sistemas e aplicações	35%	Garantir regularmente que a regra do normativo está presente em todos os logons das aplicações e sistemas	-	1	2	5	10
	Não são aplicados mecanismos de autenticação forte	Acesso ilegítimo	2	Repúdio de ações devido à conFiguração inadequada dos mecanismos de *logon*	1	Autenticação forte	-	5	25	Sistemas, equipamentos e aplicações	100%	-	-	2	1	5	25
	Os utilizadores não estão informados da sua responsabilidade por garantir que o seu nome de utilizador e palavra-chave nos sistemas são pessoais e intransmissíveis	Acesso ilegítimo	1	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	3	Divulgação de boas práticas quanto à preservação das senhas	-	5	15	Utilizadores	90%	Notificações para relembrar as boas práticas a meio dos períodos de 3 meses de mudança de *password*	-	1	1	5	5
						Informar que credenciais são intransmissíveis					90%						
	Os utilizadores não têm a possibilidade de alterar a sua palavra-chave	Acesso ilegítimo	1	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	1	-	-	5	5	Utilizadores	0%	-	-	1	1	5	5

PLAN		DO									CHECK		ACT		Resultados			
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos		Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
Função	Potenciais Modos de Falha					Prev.	Det.											
	O sistema de gestão de palavra-chave não garante a qualidade das mesmas	Acesso ilegítimo	1	Comprometimento de passwords por incumprimento das regras de composição e renovação da mesma	1	Autenticação forte	-	5	5	Sistemas, equipamentos e aplicações	100%		-	-	1	1	5	5
	O sistema não garante a renovação da palavra-chave periodicamente	Acesso ilegítimo	2	Comprometimento de passwords por incumprimento das regras de composição e renovação da mesma	1	-	Renovação automática de *password*	1	2	Sistemas, recursos de TI e aplicações	100%		-	-	2	1	1	2
	Não se recorre a procedimentos de identificação, autenticação e autorização para restringir e controlar a utilização de utilitários de sistema	Acesso ilegítimo/ indevido a utilitários de sistema	3	Acesso ilegítimo por incorreta restrição de utilizadores	1	Implementar mecanismos de controlo de acessos aos sistemas de informação	-	5	15	Sistemas, recursos de TI e aplicações	90%		Sistema de deteção de falhas dos mecanismos implementados	-	3	1	1	3
	Não está garantido que só um número restrito de utilizadores formalmente autorizados tem acesso a utilitários	Acesso ilegítimo	3	Acesso ilegítimo devido à inexistência de autorização formal de acesso aplicável aos utilitários de sistema	1	Procedimentos para a atribuição e gestão Restringir acesso de utilizadores	Revisão de acessos	2	6	Sistemas, recursos de TI e processos de Negócio	80% 100%	65%	Atualizar procedimentos de 2 em 2 anos	Revisão regular na secção de registos de acessos a utilitários	3	1	1	3
	Todos os utilitários e software de sistema desnecessários não são removidos nem bloqueados	Aumento da superfície de ataque	1	*Cyber* ataques devido à não remoção ou bloqueio aplicável aos utilitários e software de sistema	5	Remoção de utilizadores desnecessários	Mecanismos automáticos de revogação de users inativos	1	5	Aplicações	100%		-	-	1	5	1	5
	São feitas alterações não autorizadas ao código fonte de programas, controlando os acessos ao mesmo, ao desenho, às especificações, aos planos de verificação e de validação	Acesso não	2	Alteração do código fonte não autorizada devido a pobre controlo de acessos	2	-	Revisão do código fonte Controlo de acesso ao código fonte	1	4	Programas e sistemas	30% 95%		Programar revisão ao código fonte regular	-	2	1	1	2
	O código fonte não é armazenado de forma segura, numa localização central, com acesso controlado	Armazenado em localização inapropriada ou de forma insegura	3	Alteração do código fonte não autorizada devido a pobre controlo de acessos	1	Proteger código fonte	-	5	15	Programas e sistemas	100%		-	-	3	1	5	15
	Não é evitada a manutenção das bibliotecas de código fonte nos sistemas distribuídos	Acesso ilegítimo	2	Alteração do código fonte não autorizada devido a pobre controlo de acessos	4	Evitar manutenção do código fonte	-	5	40	Programas e sistemas	20%		Criar procedimento de autorização de manutenção do código fonte	Estabelecer critéris de permição de aesso automáticos	2	3	2	12
	Não é mantido um registo dos acessos às bibliotecas de código fonte dos programas	Repúdio de ações	1	Alteração do código fonte não autorizada devido a pobre controlo de acessos	3	Registar acesso à biblioteca do código fonte	Verificação de registo de entradas nas bibliotecas de código fonte dos programas	2	6	Programas e sistemas	30%	45%	Selecionar responsável por registo	-	1	2	1	2
	Não se encontram definidos os procedimentos formais para controlar a atribuição de acessos aos serviços e sistemas de Informação, que garantam uma adequada segregação de funções, quando aplicável, em conformidade com a matriz de risco adotada pelo Grupo EDP	Acessos indevidos	1	Acessos indevidos devido à inexistência de procedimentos formais para controlar a atribuição de acessos	1	Procedimentos para a atribuição, gestão e revisão de acessos	-	5	5	Procedimentos formais	85%		Divulgação e partilha de procedimentos às entidades responsáveis	Verificação de cumprimento normativo	1	1	3	3
	Os procedimentos não abrangem todas as fases do ciclo de vida do acesso do utilizador	Acessos desajustados às funções atuais	1	Acessos indevidos devido à inexistência de procedimentos formais para controlar a atribuição de acessos	4	Prodecimentar acessos	-	5	20	Procedimentos formais	70%		Reformulação específica à estruturação do ciclo de vida de acesso do utilizador	-	1	2	5	10
	A atribuição de perfis de acesso privilegiados não dispões de avaliação segundo critérios mais restritos	A atribuição indevida de perfis de acesso privilegiados	2	Acesso ilegítimo por errada gestão dos acessos privilegiados	1	Avaliar a atribuição de perfis de acesso privilegiados	-	5	10	Sistemas, recursos de TI e processos de Negócio	100%		-	-	2	1	5	10
	Não existe um processo formal para gestão dos acessos dos utilizadores aos sistemas	Acesso não autorizado ou indevido	1	Acesso ilegítimo por errada gestão dos acessos privilegiados	1	Procedimentar a gestão dos utilizadores aos sistemas	Verificação sazonal da validade do processo formal	1	1	Procedimentos formais	100%	100%	-	-	1	1	1	1
	Não se encontra assegurada a comunicação das regras e responsabilidades na utilização dos sistemas de informação do Grupo EDP a colaboradores internos e de entidades externas ao lhes ser atribuído qualquer acesso aos sistemas	Uso inadequado dos sistemas de informação do Grupo	1	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	4	Comunicação das responsabilidades de utilização dos sistemas	Método automáticos de teste sobre o entendimento da informação recebida	2	8	Utilizadores	100%	0%	Motivar a resposta aos indicadores	Teste e prática do método desenvolvido	1	3	1	3

PLAN		DO									CHECK		ACT		Resultados			
Identificação						Controlos												
Função	Potenciais Modos de Falha	Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Prev.	Det.	DET	RPN	Tipo de Ativos	Efetividade dos Controlos		Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
	Para cada sistema não estão identificados o conjunto de perfis e privilégios, que são alocados aos utilizadores conforme a necessidade	Acesso indevido	**2**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**2**	Identificar perfis e privilégios	Verificação de alocações de perfis e privilégios regular	**2**	**8**	Sistemas, recursos de TI e aplicações	100%	55%	Garantir que a verificação abrange todo o Grupo EDP inclusive os serviços de entidades externas	-	**2**	**1**	**2**	**4**
	Os privilégios de acesso aos sistemas que são atribuídos aos colaboradores e entidades externas não tem em consideração as necessidades efetivas para o desempenho das funções	Acesso indevido	**1**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**1**	-	-	**5**	**5**	Sistemas, recursos de TI e processos de Negócio	0%		-	Estabelecer controlos efetivos para o princípo enunciado	**1**	**1**	**5**	**5**
	Os privilégios de acesso aos sistemas não garantem uma correta segregação de funções ou não estão implementados os controlos compensatórios adequados	Acesso indevido	**1**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**1**	-	-	**5**	**5**	Sistemas, recursos de TI e processos de Negócio	0%		Implementados os controlos compensatórios adequados	Garantir correta segregação de funções sistemática	**1**	**1**	**3**	**3**
	Solicitações de atribuição ou alteração de privilégios de acesso aos sistemas não são formalmente colocadas no sistema de gestão de Identidades e acessos	Falta de monitorização	**1**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**3**	Registar solicitações de privilégios	-	**5**	**15**	Programa de registo processual	100%		Mecanismos de deteção de alterações não solicitadas	-	**1**	**2**	**2**	**4**
	Os pedidos de criação, alteração e revogação de acessos de qualquer utilizador não se encontram registados pelos responsáveis desta função no Negócio e, posteriormente aprovados	Falta de monitorização	**1**	Acesso privilegiado ilegítimo por falta de aprovação	**3**	Aprovação de pedidios de acesso	Processo de verificação de aprovações	**3**	**9**	Sistemas, recursos de TI e aplicações	75%	90%	Implementar processode verificação	-	**1**	**1**	**1**	**1**
	Os acessos e respetivos privilégios são implementados nos sistemas antes de obtidas todas as aprovações necessárias	Desconhecimento dos acessos e respetivos privilégios	**2**	Acesso privilegiado ilegítimo por falta de aprovação	**1**	-	Implementar acessos e privilégios após aprovação	**1**	**2**	Sistemas, recursos de TI e aplicações	100%		-	-	**2**	**1**	**1**	**2**
	Não é mantido um registo formal de todos os utilizadores autorizados e respetivos privilégios de acessos aos sistemas do Grupo EDP	Falta de monitorização	**2**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**1**	Registo de utilizadores autorizados e respetivos privilégios	-	**5**	**10**	Programa de registo processual	100%		Responsabilizar colaboradores pela manutenção de registos de privilégios	Verificação trimestral da coerência dos registos	**2**	**1**	**2**	**4**
	Os privilégios de acesso aos sistemas disponibilizados aos colaboradores não são revogados, de forma automática, assim que termina a sua relação profissional com o Grupo EDP	Acesso indevido	**1**	Acesso privilegiado ilegítimo por falta de revogação	**1**	Revogação automática de privilégios a ex-colaboradores	-	**5**	**5**	Sistemas, recursos de TI e aplicações	100%		-	-	**1**	**1**	**5**	**5**
	Não é feita uma revisão periódica com vista à remoção ou bloqueio de contas redundantes e/ou desnecessárias	Acesso aos sistemas através de contas redundantes e/ou desnecessárias	**3**	*Cyber* ataques devido à não remoção ou bloqueio aplicável aos utilitários e *software* de sistema	**1**	-	-	**5**	**15**	Sistemas, recursos de TI e processos de Negócio	0%		-	Revisão periódica com vista à remoção ou bloqueio de contas redundantes e/ou desnecessárias	**3**	**1**	**2**	**6**
	Os colaboradores e entidades externas não têm associados, identificadores individuais (user ID), protegidos por *password*	Não identificação dos autores dos acessos/atividades	**3**	Acesso ilegítimo por errada gestão dos acessos privilegiados	**1**	ID único protegido por *password* para cada colaborador	Sistema de deteção de ID sem *password*	**1**	**3**	Sistemas, recursos de TI e aplicações	100%	100%	-	-	**3**	**1**	**1**	**3**
	A utilização de identificadores genéricos (contas genéricas ou de grupo) não requer permissões	Não identificação dos autores dos acessos/atividades	**1**	Utilização de identificadores genéricos injustificada por falta de controlo e monitorização	**4**	Aprovar e registar identificadores genéricos	-	**5**	**20**	Sistemas, recursos de TI e aplicações	100%		-	-	**1**	**4**	**5**	**20**
	Cada conta genérica não tem associado um utilizador individual responsável por essa mesma conta	Não identificação dos autores dos acessos/atividades	**1**	Utilização de identificadores genéricos injustificada por falta de controlo e monitorização	**2**	Atribuir utilizador individual a conta genérica	Automatização do processo de criação de contas genéricas com permissão apenas após a associação de um responsável	**3**	**6**	Sistemas, recursos de TI e aplicações	30%	40%	-	Implementação dos controlos a todas as aplicações	**1**	**2**	**1**	**2**
	A nomenclatura utilizada na geração dos identificadores não está em concordância com as regras definidas pelo Grupo EDP	Não identificação do grupo ao qual pertence user ID	**1**	Não identificação do grupo ao qual pertence user ID devido ao incuprimento regras de gestão de acessos	**1**	Cumprir regras de nomenclatura de user IDs	-	**5**	**5**	Sistemas, recursos de TI e aplicações	15%		Verificar o funcionamento de automatismo de aceitação de credenciais	Automatizar eurísticas de geração de identificadores	**1**	**1**	**1**	**1**
	O Grupo EDP define regras que regulem a nomenclatura a adotar na criação de user IDs	Não identificação do grupo ao qual pertence user ID	**1**	Não identificação do grupo ao qual pertence user ID devido ao incuprimento regras de gestão de acessos	**2**	Procedimentar a geração dos identificadores	-	**5**	**10**	Documento normativo	0%		Determinar responsável por procedimentar a geração dos identificadores	-	**1**	**2**	**3**	**6**

PLAN		DO									CHECK		ACT		Resultados			
Identificação						Controlos												
Função	Potenciais Modos de Falha	Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Prev.	Det.	DET	RPN	Tipo de Ativos	Efetividade dos Controlos		Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
	O identificador não é pessoal, de utilização exclusiva nem único para todos os sistemas	Possibilidade de negação de autoria de atividades, devido ao user ID ser partilhado Comprometimento da eficiência do rastreamento de atividades	1	Acesso ilegítimo por errada gestão dos acessos privilegiados	1	-	-	5	5	Sistemas, recursos de TI e aplicações	0%		-	-	1	1	5	5
	Os identificadores pertencentes a colaboradores do Grupo EDP que já não têm um vínculo contratual com o Grupo EDP são atribuídos a outros colaboradores	Possibilidade de negação/ repúdio de autoria de atividades	1	Possibilidade de negação/ repúdio de autoria de atividades, devido ao user ID não estar formalmente atribuído a uma pessoa	1	Impossibilitar a reutilização de identificadores	-	5	5	Sistemas, recursos de TI e aplicações	0%		Automatizar um processo que impossibilite a reutilização de identificadores	-	1	1	1	1
	O Grupo EDP não exerce o direito de, sem aviso prévio, bloquear, suspender, alterar e monitorizar os utilizadores dos seus sistemas e respetivos privilégios de acesso	Comprometimento da rede do Grupo EDP	2	Acesso privilegiiado ilegítimo por falta de revogação	3	-	-	5	30	Sistemas, recursos de TI e processos de Negócio	0%		-	-	2	3	5	30
	A autorização do acesso não é efetuada pelo dono do ativo de informação	Desconhecimento do dono do ativo que determinado user ID tem acesso ao ativo	1	Direitos de acesso injustificáveis por falta de autorização do dono do ativo	1	Autorização de acesso é feita pelo dono do ativo	-	5	5	Ativos de informação	100%		-	-	1	1	5	5
	Os direitos de acesso são disponibilizados antes da autorização do dono do ativo	Desconhecimento do dono do ativo que determinado user ID tem acesso ao ativo	1	Direitos de acesso injustificáveis por falta de autorização do dono do ativo	3	Direito de acesso disponibilizados após autorização	-	5	15	Ativos de informação	35%		Integração de SIEM e IAM	Comunicação automática com o dono do ativo	1	2	3	6
	Inexistência de um registo centralizado dos direitos de acessos concedidos	Ineficiente revisão dos direitos de acesso	1	Ineficiente revisão dos direitos de acesso devido aos mesmos estarem em várias localizações	1	Registar direitos de acesso automaticamente	-	5	5	Programa de registo centralizado	90%		-	Integrar todos os sistemas das geografias EDP	1	1	5	5
	Alterações à condição profissional dos colaboradores, que envolvam alteração das necessidades efetivas de acesso aos sistemas, não se encontram refletidas nos acessos e privilégios disponibilizados	Acesso indevido a sistemas / funcionalidades	1	Repúdio de ações por falta de direitos de acesso ou ações acidentais por uso errado de direitos de acesso	5	Atualização de direitos de acesso	Deteção automática de alterações de carreira	2	10	ID Utilizadores	70%	70%	Integração entre os mecanismos de deteção e a atualização de direitos de acesso	-	1	3	2	6
	Os acessos privilegiados não obedecem a todas as regras definidas nesta Norma e, adicionalmente, não são alvo de avaliação caso a caso, pela área responsável pela segurança da informação. Estes acessos não se encontram identificados nem registados.	Acesso indevido a sistemas / funcionalidades	4	Acesso ilegítimo por errada gestão dos acessos privilegiados	1	Acessos priviligiados coerentes com a NO-SI-006 Registar acessos priviligiados	Avaliação dos acessos priviligiados pela área de Segurança da Informação	2	8	Programa de registo processual e documento normativo	100% 100%	50%	Responsabilizar colaboradores pela manutenção de registos de privilégios	Verificação trimestral da coerência dos registos	4	1	1	4
	Os utilizadores com acessos privilegiados recorrem às suas contas privilegiadas em atividades normais de utilizador, enquanto que estas devem ser realizadas através das suas contas regulares	Ações acidentais ou não intencionais com impacto na organização	1	Ações acidentais por uso errado de acessos privilegiados	5	Formação sobre a correta utilização de privilégios	-	5	25	Sistemas, recursos de TI, equipamentos e aplicações	100%		-	-	1	5	5	25
	Os acessos atribuídos no âmbito de operações extraordinárias não têm um período de validade máxima de 24 horas em ambientes produtivos e 72 horas em ambientes não produtivos	Ações acidentais ou não intencionais com impacto na organização	1	Ações acidentais por uso errado de acessos privilegiados	1	-	Restrição de acessos aos ambientes não produtivos Validade dos acessos em operações extraordinárias	1	1	Sistemas e equipamentos	100% 100%		-	-	1	1	1	1
	Alterações a acessos e contas privilegiadas não são registados no sentido de permitir a sua revisão	Desconhecimento de alterações a acessos e a contas privilegiadas	1	Acesso ilegítimo por errada gestão dos acessos privilegiados	3	Registar alterações a acessos e contas priviligiados	Rever alterações a acessos e contas priviligiados	5	15	ID Utilizadores	20%	20%	Responsabilizar colaboradores pela manutenção de registos de privilégios	Verificação trimestral da coerência dos registos com as alterações efetuadas	1	2	4	8
	Não é assegurada a comunicação das regras e responsabilidades na utilização das *passwords* de acesso aos sistemas de informação do Grupo EDP	Uso inadequado das *passwords*	2	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	1	-	-	5	10	Utilizador	0%		Garantir comunicação	Testar transmissão de conhecimento	2	1	4	8
	Não se encontra estabelecido um procedimento de validação da identidade do utilizador antes de lhe ser atribuída uma nova *password* ou uma *password* de substituição ou temporária	Usurpação de identidade do utilizador	2	Usurpação de identidade do utilizador por inexistência de procedimento de validação	1	Procedimentar a validação da identidade	-	5	10	Documento normativo	100%		-	-	2	1	5	10

PLAN		DO									CHECK	ACT		Resultados			
Identificação		Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Controlos		DET	RPN	Tipo de Ativos	Efetividade dos Controlos	Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
Função	Potenciais Modos de Falha					Prev.	Det.										
	As *passwords* utilizadas nos sistemas do Grupo EDP não obedecem a regras de composição, estas não são verificadas automaticamente sempre que os utilizadores alterem a sua password	Comprometimento de *passwords*	3	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	2	Implementar regras de definição e renovação de senhas Procedimentar a definição e renovação das senhas	-	5	30	Sistemas, recursos de TI, equipamentos e aplicações	90% 100%	Integração de SIEM e IAM	-	3	1	5	15
	As novas *passwords* atribuídas aos utilizadores e as passwords de substituição ou temporárias não são únicas para um utilizador	Comprometimento de *passwords*	1	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	1	Singularidade das novas *passwords*	-	5	5	Sistemas, recursos de TI, equipamentos e aplicações	100%	-	-	1	1	5	5
	As *passwords* atribuídas administrativamente aos utilizadores não expiram automaticamente no momento da primeira tentativa de autenticação com sucesso	Comprometimento da *password*	2	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	1	*Password* expira autimaticamente aquando alteração	-	5	10	Sistemas, recursos de TI, equipamentos e aplicações	100%	-	-	2	1	5	10
	As *passwords* dos utilizadores não expiram periodicamente, obrigando à respetiva alteração	Utilização de *passwords* comprometidas	2	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	1	Repor a *password* periodicamente	-	5	10	Sistemas, recursos de TI, equipamentos e aplicações	100%	-	-	2	1	5	10
	Inexistência de limitações à reutilização de *passwords*	Utilização de *passwords* comprometidas	4	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	2	Implementar regras de definição e renovação de senhas Limitar a reutilização de *passwords*	-	5	40	Sistemas, recursos de TI, equipamentos e aplicações	90% 100%	Integração de SIEM e IAM	-	4	1	5	20
	Um utilizador pode proceder a mais do que uma alteração de *password* dentro de um período de tempo definido	Alteração frequente de *password* até ser possível utilizar a mesma (podendo esta estar comprometida)	1	Comprometimento de *passwords* por incumprimento das regras de composição e renovação da mesma	1	Impedir alteração da *password* dentro de um período de tempo definido	Cronometrar a última alteração e a sua validade automaticamente	1	1	Sistemas, recursos de TI, equipamentos e aplicações	100%	-	-	1	1	1	1
	A visualização das *passwords* não está mascarada, suprimida ou, de alguma forma, protegida da observação de terceiros	Comprometimento de *passwords*	2	Revelação de informações sobre o sistema devido à inexistência de mecanismos de ocultação	1	Mascarar *password*	-	5	10	Equipamentos	100%	-	-	2	1	5	10
	As *passwords* são guardadas nos sistemas de forma desprotegida	Comprometimento de *passwords*	1	Comprometimento de *passwords* devido à proteção inadequado da mesma	1	*Passwords* não são guardadas no sistema	-	5	5	Sistemas TI	100%	-	-	1	1	5	5
	São permitidas *passwords* embebidas no código das aplicações e sistemas	Comprometimento de *passwords*	1	Comprometimento de *passwords* devido à proteção inadequado da mesma	1	Recusar *passwords* embebidas no código das aplicações e sistemas	-	5	5	Sistemas, recursos de TI, equipamentos e aplicações	100%	-	-	1	1	5	5
	Os acessos dos utilizadores não são revistos de acordo com o processo de revisão de identidades e acessos, não garantindo que os acessos atribuídos continuam a ser adequados	Desatualização dos acessos dos utilizadores	1	Cyber ataques devido à não remoção ou bloqueio aplicável aos utilitários e *software* de sistema	4	-	-	5	20	-	0%	-	Auditar a revisão de acessos dos utilizadores	1	3	5	15
	A revisão de identidades e acessos não é efetuada de forma a garantir que apenas estão ativas as identidades de colaboradores no ativo e que os acessos aprovados são os efetivamente atribuídos e os estritamente necessários para a execução das funções dos colaboradores	Acesso indevido aos sistemas	1	Acesso ilegítimo por incorreta restrição de utilizadores Cyber ataques devido à não remoção ou bloqueio aplicável aos utilitários e *software* de sistema	4	-	-	5	20	-	0%	-	Auditar a revisão de acessos dos utilizadores	1	3	5	15
	Os acessos implementados nos sistemas não se encontram sujeitos a um processo automático de monitorização contínua que permita detetar/corrigir incoerências com os acessos aprovados	Acessos implementados diferentes dos que foram aprovados	2	Acessos implementados diferentes dos que foram aprovados devido à inexistência de um processo automático de monitorização contínua	3	-	Monitorização e automaticamente dos acessos implementados	1	6	Sistemas, recursos de TI, equipamentos e aplicações	85%	Monitorização contínuamente e automaticamente dos acessos implementados	-	2	1	1	2

PLAN		DO									CHECK		ACT		Resultados			
Identificação						Controlos												
Função	Potenciais Modos de Falha	Potenciais Efeitos das Falhas	GRAV	Mecanismos de Falha / Causas	OCUR	Prev.	Det.	DET	RPN	Tipo de Ativos	Efetividade dos Controlos		Ações de Melhoria	Ações de Correção	GRAV	OCUR	DET	RPN
	Sempre que um contrato termina ou é modificado, não é considerada a remoção ou modificação dos acessos atribuídos a esses colaboradores ou entidades externas	Acesso indevido	**1**	Repúdio de ações por falta de direitos de acesso ou ações acidentais por uso errado de direitos de acesso	**5**	-	-	**5**	**10**	ID Utilizadores	0%		Definir responsável por considerar a remoção ou modificação dos acessos atribuídos a colaboradores ou entidades externas	Notificar automaticamente sempre que ocorram alterações de carreira em todo o Grupo EDP	**1**	**2**	**2**	**4**
	Os utilizadores não conhecem nem cumprem com as suas responsabilidades, particularmente no que respeita à utilização de credenciais de acesso e à Segurança da Informação na utilização dos acessos que lhes foram atribuídos	Comprometimento do acesso à informação	**5**	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	**1**	-	-	**5**	**25**	Utilizadores	0%		Formação sobre responsabilidades de utilização de credenciais de acesso e de Segurança da Informação na utilização dos acessos Teste dos conhecimentos	Reenforço regular do foco da formação	**4**	**1**	**3**	**12**
	Os utilizadores não mantem as suas credenciais de acesso confidenciais	Comprometimento das credenciais de acesso	**5**	Acesso indevido por desconhecimento das regras da norma de controlo de acessos	**2**	-	-	**5**	**50**	Utilizadores	0%		Formação sobre responsabilidades de utilização de credenciais de acesso e de Segurança da Informação na utilização dos acessos Teste dos conhecimentos	Reenforço regular do foco da formação	**5**	**1**	**3**	**15**
	Os utilizadores não alteram as suas credenciais de acesso sempre que existe informação do possível comprometimento destas ou dos sistemas em que são utilizadas	Utilização de credenciais de acesso comprometidas ou sistemas onde elas são utilizadas também comprometidos	**5**	Utilização de credenciais de acesso comprometidas ou sistemas onde elas são utilizadas também comprometidos devido à não alteração das credenciais	**1**	Alterar credenciais sempre que estejam comprometidas	-	**5**	**25**	Utilizadores	10%		Comunicar sempre que haja comprometimento online de *passwords* detetado	-	**5**	**1**	**2**	**10**
	Os utilizadores não criam nem alteram as suas *passwords* de acordo com as regras definidas pelo Grupo EDP	*Passwords* com reduzida complexidade ou alteradas de forma inadequada	**1**	Comprometimento de credenciais de acesso devido à utilização de protocolos inseguros aplicáveis aos sistemas e aplicações	**1**	*Password* gerida pelo IAM (AD)	Mecanismos automáticos de aceitação apenas por cumprimento das regras das *passwords*	**2**	**2**	Utilizadores	90%	100%	Integração IAM a todas as aplicações geridas pelo Grupo EDP, incluindo geografias	-	**1**	**1**	**1**	**1**
	Os utilizadores incluem as *passwords* em processos automáticos por exemplo, numa macro ou função	Comprometimento das *passwords*	**2**	Comprometimento de *passwords* devido à proteção inadequado da mesma	**4**	Impedir a inclusão de *passwords* em processos automáticos	-	**5**	**40**	Utilizadores	100%		-	-	**2**	**1**	**5**	**10**
	Os utilizadores partilham as *passwords* de contas de grupo para fora dos elementos pertencentes ao mesmo	Comprometimento das *passwords* de contas de grupo	**1**	Comprometimento de *passwords* devido à proteção inadequado da mesma	**2**	Comunicar os perigos de partilha de *passwords*	-	**5**	**10**	Utilizadores	75%		Formação sobre responsabilidades de salvaguarda de *passwords* Teste dos conhecimentos	Reenforço regular do foco da formação	**1**	**1**	**4**	**4**
	Os utilizadores utilizam as mesmas *passwords* para uso pessoal e profissional	Comprometimento das *passwords* de uso profissional	**3**	Comprometimento de *passwords* devido à proteção inadequado da mesma	**3**	-	-	**5**	**45**	Utilizadores	0%		Formação sobre responsabilidades de salvaguarda de *passwords* Teste dos conhecimentos	Reenforço regular do foco da formação	**3**	**2**	**4**	**30**
	As *passwords* associadas a identificadores partilhados ou a equipamentos específicos, que são do conhecimento de colaboradores ou entidades externas que deixaram de exercer as funções ou cujos contratos terminaram, não são alteradas	Conhecimento de *passwords* por parte de colaboradores ou entidades externas que deixaram de exercer as funções ou cujos contratos terminaram	**2**	Utilização de credenciais de acesso comprometidas ou sistemas onde elas são utilizadas também comprometidos devido à não alteração das credenciais	**1**	Alterar *passwords* partilhadas com ex-colaboradores	Deteção automática de alterações de carreira	**2**	**4**	Sistemas, recursos de TI, equipamentos e aplicações	100%	70%	Integração entre os mecanismos de deteção e a validação de credenciais	-	**2**	**1**	**1**	**2**

⟨2021⟩

ANA SOFIA MARQUES LOPES DE MATOS

GESTÃO DE RISCO E CONFORMIDADE EM TECNOLOGIAS DA INFORMAÇÃO SEGUNDO A ABORDAGEM GRC

NOVA SCHOOL OF SCIENCE & TECHNOLOGY